UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"AUDITORÍA PARA EVALUAR LA SEGURIDAD FÍSICA DEL DATA CENTER DEL HOSPITAL REGIONAL DE AYACUCHO, 2019"

Tesis presentado por	**:**	Abel Vilca Dipaz
Para optar el Título Profesional de	**:**	Ingeniero de Sistemas
Tipo de Investigación	**:**	Observacional, Prospectiva, Transversal y descriptivo
Área de Investigación	**:**	Auditoría informática
Asesor	**:**	Ing. Karel PERALTA SOTOMAYOR

Ayacucho, noviembre 2019

DEDICATORIA

A mis padres por apoyarme día a día en mi crecimiento como persona y profesionalmente. Por todo el apoyo brindado y que confiaron en mi a pesar de tantas dificultades.

A mis hermanos, por haber fomentado en mí el deseo de seguir estudiando frente a cualquier limitación.

A mis amigos que compartieron las experiencias, consejos y los años de aprendizaje.

Muchas gracias por todo.

AGRADECIMIENTO

A Dios por darme la vida, salud y fortaleza para cumplir con esta meta.

A la Universidad Nacional de San Cristóbal de Huamanga, mi alma máter que me dio la oportunidad de una educación superior de calidad y en la cual he forjado los conocimientos profesionales día a día.

A todos los profesores que me enseñaron con amor y dedicación compartieron sus conocimientos para desempeñar con satisfacción mi profesión. En especial al Ing. Karel, por la paciencia y dedicación brindada para realizar un buen trabajo.

A los trabajadores del Área informática del Hospital Regional de Ayacucho por dedicar su tiempo para concluir con mi investigación.

A todos mis amigos, los cuales compartimos grandes momentos en el viaje de esta carrera.

Muchas gracias por todo.

CONTENIDO

CAPÍTULO I

PLANTEAMIENTO DE LA INVESTIGACIÓN

CAPÍTULO II

REVISIÓN DE LITERATURA

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

CAPÍTULO IV

ANÁLISIS Y RESULTADOS DE LA INVESTIGACIÓN

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

RESUMEN

En toda organización el Centro de Datos tiene la misión de proteger la información más importante, son los responsables de procesar todas las transacciones de cada organización. La infraestructura donde se van a mantener y alojar los equipos del Centro de Datos es muy importante, ya que se debe determinar las mejores condiciones físicas y ambientales para su preservación, mismas que deberán estar definidas bajo normas como: NTP-ISO/IEC 17799. Además, es importante también considerar aspectos como: las amenazas, riesgos y vulnerabilidades de la seguridad física para evitar fugas de información o daños, en efecto desde donde se lo quiera ver un Centro de Datos es el cerebro de una organización. Sin embargo, no se cuenta con un mecanismo que permita a los clientes asegurar que su información es almacenada de la mejor manera.

El objetivo de este trabajo de investigación es diseñar procedimientos de auditoría para evaluar la seguridad física del Data Center del Hospital Regional de Ayacucho, mediante el marco de control COBIT 5.0 y la norma técnica peruana NTP-ISO/IEC 17799. El tipo de investigación es observacional, prospectivo, transversal y descriptivo.

Palabras claves: Auditoría en seguridad Física, Riesgo, Amenaza, COBIT 5.0, Análisis de Riesgo, criterios de seguridad y La Norma Técnica Peruana NTP-ISO/IEC 17799.

INTRODUCCIÓN

En el desarrollo de la presente investigación se define los procedimientos de Auditoría de seguridad física, se empleará el marco de control COBIT 5.0 que tienen relación directa con la seguridad física, y La Norma Técnica Peruana NTP-ISO/IEC 17799, Con estos procedimientos se permitirán recoger, agrupar y evaluar evidencias para determinar si las instalaciones del Data Center salvaguardan la información que procesa, y utiliza adecuadamente sus recursos.

Actualmente el Data Center del Hospital Regional de Ayacucho no cuenta con ningún procedimiento de auditoría, y por lo tanto se plantea los siguientes problemas: ¿De qué manera los activos físicos están implicados en la seguridad física del Data Center del Hospital Regional de Ayacucho?; ¿Cuáles son las Amenazas y riesgos comunes que atentan contra los activos físicos del Data Center de Hospital Regional de Ayacucho?; ¿Cómo evaluar los activos físicos mediante los criterios de seguridad física en el Data Center del Hospital Regional de Ayacucho?.

Y sus posibles soluciones con los siguientes: a) Identificar y planear la seguridad de los activos físicos implicados en la seguridad Física del Data Center del Hospital Regional de Ayacucho, b) Mencionar cuáles son las amenazas y riesgos comunes que atentan contra los activos físicos del Data center del Hospital Regional de Ayacucho; c) Evaluar los activos físicos mediante criterios de seguridad física basada en controles de COBIT 5.0 y la NTP-ISO/IEC 17799, del Data center del Hospital Regional de Ayacucho.

CAPÍTULO I

PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 DIAGNÓSTICO Y ENUNCIADO DEL PROBLEMA

Hoy por hoy vivimos en una sociedad donde uno de los principales activos de cualquier organización, institución o empresa es la información, no importa su tamaño o giro del negocio. A nivel mundial la auditoría informática constituye un pilar fundamental en las organizaciones, porque tanto los sistemas como las estructuras físicas deben estar sometidos a controles de calidad. En la actualidad este enfoque es necesario para poder alertar a las empresas de la importancia que tiene la protección de sus equipos de Data center, para prevenir o evitar daños físicos.

International Computer Room Experts Association (ICREA), el principal riesgo de seguridad en los Data Centers mexicanos es el error humano. El especialista Rocha, Eduardo; explicó que las situaciones de riesgo en más del 95% de los casos obedecen a errores humanos que son involuntarios, aunque a veces son dolosos. “Una buena operación debe establecer los procedimientos y tiene que mantener al día los recursos como la gestión de la energía eléctrica, la gobernabilidad o el clima. Pero el verdadero reto, y a veces minimizado por increíble que parezca, es incluir al proceso a toda la plantilla laboral que gestionará y laborará en el centro de datos. Esto involucra a todos: desde los administradores y personal técnico, operadores, personal de intendencia y seguridad (guardias)”. Lo que debe hacerse es seguir las normas internacionales que prevén ese tipo de eventos, ya que actúan como referente para la construcción de centros de datos: "Las normativas hacen énfasis en los niveles de seguridad (física e informática) y eficiencia”, comentó Rocha. y según la web América sistemas 2016, El mercado de Centros de Datos en el Perú está aún en desarrollo, un desarrollo más lento de lo esperado sobre todo en el sector público; el mercado no se ha desarrollado adecuadamente debido a la falta de conocimiento especializado en diseño, eficiencia energética, enfriamiento, administración de infraestructura y operaciones críticas. Otro de los problemas presentados es la improvisación del desarrollo de sus instalaciones, las cuales las hacen sin previsión y planeamiento instalando equipos con poco criterio de diseño y luego readecuando o rediseñando complicando con ello sus operaciones.

Figura N° 1 Data center de Google. (Google, 2018)

Por ello, considerando que el área de informática en específico el área de Data center del Hospital Regional de Ayacucho, es una entidad estatal que brinda servicios públicos de salud; especializada, de calidad y con tecnología actualizada. Siendo una entidad importante para la ciudad de Ayacucho. los cuales benefician a toda la población de la región y a las regiones vecinas, entre otros cuenta con importantes recursos tecnológicos, que pueden ser víctimas de amenazas, pudiendo ocasionar pérdidas económicas a la institución, por lo tanto, necesita someterse a una evaluación técnica objetiva basado en estándares internaciones, para conocer el nivel de seguridad alcanzado por sus actividades de control y mantener mecanismos de seguridad sobre ellos.

Por lo expuesto, la auditoría sobre la seguridad física, permitirá determinar el nivel de riesgo y el grado de confianza que mantienen los recursos tecnológicos del Data Center del Hospital Regional de Ayacucho, respecto a los controles de seguridad que se están utilizando, con el fin de incrementar la confiabilidad en los procesos y reducir los riesgos.

Hasta la fecha no ha sido sometida a ningún tipo de proceso o estudio de Auditoría informática para identificar las posibles falencias en la infraestructura de la seguridad física del Data Center del Hospital Regional de Ayacucho, poniéndolo de este modo como un punto blanco fácil de ataques, de pérdidas o de daños irreversibles; por tal motivo es necesario realizar un diagnóstico y calificación de sus niveles de seguridad, utilizando la auditoría como una herramienta de evaluación. Como punto central se enfocará en la seguridad física del Data Center.

1.2 FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

PROBLEMA PRINCIPAL

¿Cómo realizar una auditoría para evaluar la seguridad física del Data Center del Hospital Regional de Ayacucho?

PROBLEMAS ESPECÍFICOS

a) ¿De qué manera los activos físicos están implicados en la seguridad física del Data Center del Hospital Regional de Ayacucho?;

b) ¿Cuáles son las Amenazas y riesgos comunes que atentan contra los activos físicos del Data Center de Hospital Regional de Ayacucho?;

c) ¿Cómo evaluar los activos físicos mediante los criterios de seguridad física en el Data Center del Hospital Regional de Ayacucho?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Diseñar procedimientos de auditoría para evaluar la seguridad física del Data Center del Hospital Regional de Ayacucho, Mediante el marco de control COBIT 5.0 y la norma técnica peruana NTP-ISO/IEC 17799.

OBJETIVOS ESPECÍFICOS

a) Identificar y planear la seguridad de los activos físicos implicados en la seguridad Física del Data Center del Hospital Regional de Ayacucho;

b) Mencionar cuáles son las amenazas y riesgos comunes que atentan contra los activos físicos del Data center del Hospital Regional de Ayacucho;

c) Evaluar los activos físicos mediante criterios de seguridad física basada en controles de COBIT 5.0 y la NTP-ISO/IEC 17799, del Data center del Hospital Regional de Ayacucho.

1.4 JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN

JUSTIFICACIÓN

Los Data Center son ubicaciones en donde se localizan todos los elementos necesarios para el cálculo y procesamiento de datos de una organización, teniendo como objetivo de procesar y resguardar uno de los bienes más importantes, valiosos e irremplazables que tiene una organización, que es su información. La seguridad física en un Data Center asegura el buen funcionamiento y la disponibilidad de los procesos y de los servicios de Tecnología de Información. En efecto, surge la necesidad realizar la evaluación de la Seguridad Física en el Data Center del Hospital Regional de Ayacucho, porque aparte de verificar las falencias, se podrían aplicar controles y políticas en base a las recomendaciones obtenidas para minimizar en el futuro que ocurran estos problemas, y como una forma de prevención para el tratamiento adecuado de Datos y el cuidado de la información.

En lo social la presente investigación tiene como objetivo de hacer una auditoría en seguridad física, que colabore con la institución u organización auditada en la prevención de eventualidades no deseadas, en la definición de las futuras líneas de actuación y en la eliminación de algunos riesgos más críticos, teniendo como referencia el Data Center del Hospital Regional de Ayacucho.

El valor teórico de la propuesta de la investigación se basa en marcos de control reconocidos internacionalmente, COBIT 5.0, la norma técnica peruana NTP-ISO/IEC 17799; cuyos procesos e indicadores garantizan una evaluación certera y objetiva**.** porque aparte de verificar las falencias, se podrían aplicar controles y políticas para minimizar en el futuro que ocurran problemas, y como una forma de prevención para el tratamiento adecuado de Datos y el cuidado de la información. El Hospital Regional de Ayacucho se beneficiaría del presente trabajo, pues al verificar la capacidad y el cumplimiento de las medidas de seguridad física de su Data Center, se podría llegar a rectificaciones posteriores en sus políticas de seguridad, así como en sus controles que sean críticos y les ocasionen problemas.

DELIMITACIÓN

Esta investigación se desarrollará en el Área de Data Center del Hospital Regional de Ayacucho, con la información del año 2019. en la cual se verificará y se evaluará las condiciones de seguridad Física, tendrá un tiempo de realización de 5 Meses, de acuerdo a

las diferentes actividades a realizar durante el desarrollo del mismo. Los conceptos que se van a manejar en este proyecto se van a relacionar con la Seguridad Física del Data Center basados en marco de control COBIT, la norma técnica peruana NTP-ISO/IEC 17799, en esta investigación no se tomará en cuenta la seguridad Lógica.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

Según Loor & Espinoza (2015), en su tesis "Auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la espam mfl", concluyeron que la aplicación de técnicas en auditoría, resultaron de gran utilidad, y la ausencia de una normativa de seguridad para una adecuada evaluación y control de los recursos de TI, trae como consecuencias que estos operen en ambientes poco seguros y confiables.

(Tongo, 2017), en la tesis "Diagnóstico situacional del Data Center bajo cumplimiento normativo y de estándar en el Hospital II ESsalud de Huaraz" concluye, con la descripción del diagnóstico situacional de Data center se logró identificar controles tanto de estandarización y normalización que se deben de tener en cuenta al planificar el diseño de un Data Center, lo cual ayudara a futuras investigaciones e implementación de un data center.

(Marulanda, 2014) en sus tesis "Evaluación mediante el estándar ISO 27001 de la seguridad Física y Lógica de la infraestructura tecnológica de la clínica san José S.A.S de la ciudad de Barranca Bermeja – Santander" afirma que la auditoría informática se encarga de gestionar y evaluar las vulnerabilidades que pudieran estar presentes en los sistemas de información. Una vez enfocada las inconsistencias de las empresas se documentan, se reportan los resultados a los gerentes o responsables de las instalaciones y se sugieren medidas que permitan mejorar la seguridad.

(Huerta, 2015) en su tesis "Procedimientos para la auditoría en seguridad física del Data Center de la Municipalidad Provincial de Huamanga", concluye Los procedimientos de auditoría en seguridad física, incluyen en una de sus etapas, el análisis de riesgo, con ello se alcanza identificar los riesgos que ponen en peligro la continuidad y disponibilidad de un Data Center, en concreto del Data Center de la MPH.

(Aguirre & Palacios, 2014), en su investigación "Evaluación técnica de seguridades del Data Center del Municipio de Quito según las Normas ISO/IEC 27001:2005 SGSIE ISI/IEC 27002:2005." Concluyen que al no realizar auditorías a los procesos de seguridad no se posee una idea clara de cómo se encuentran y el estado de cumplimiento si se ha mejorado o empeorado el cumplimiento de los controles, también La falta de un Data Center alterno puede ser la causa de que, si se da un evento fortuito con el Data Center, se tenga tiempos muy altos o en el peor de los casos catastróficos la restauración de los servicios para la atención al público.

2.2 MARCO TEÓRICO

2.2.1 Seguridad Física

Según (Seoane, Saiz, Fernández, & Fernández, 2010) La seguridad física es aquella que trata de proteger el hardware (los equipos informáticos, el cableado ...) de los posibles desastres naturales (terremotos, tifones ...), de incendios, inundaciones, sobrecargas eléctricas, de robos y un sinfín de amenazas más. Los planes de seguridad física se basan en proteger el hardware de los posibles desastres naturales, de incendios, inundaciones, sobrecargas eléctricas, robos y otra serie de amenazas.

Para (Costas, 2011) Así, la seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad, dentro y alrededor de la ubicación física de los sistemas informáticos, así como los medios de acceso al mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Según (Roa, 2013). La seguridad física cubre todo lo referido a los equipos informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red. Las amenazas contra la seguridad física son: desastres naturales, robos y fallos de suministros.

Para (Piattini & Del peso, 2001), La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un CPD. Si se entiende la contingencia o proximidad de un dato como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación con la cronología del fallo: antes durante y después.

La Seguridad Física para (Huerta Villalón, 2000) consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Datos, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2.2.2 Auditoría en Seguridad Física

"Conceptualmente la Auditoría, toda y cualquier Auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad general más que en el Alcance de la misma que pretende reflejar y/o cumple las condiciones que le han sido prescritas", La Auditoría Física, interna o externa, no es sino una auditoría parcial, por lo que difiere de la auditoría (Piattini & Del peso, 2001).

"La auditoría de la seguridad física analiza todos los procesos referentes a la protección de los componentes hardware, dispositivos, instalaciones y entornos de los distintos sistemas informáticos. Los auditores deberán analizar la correcta protección y actualización de estos componentes, además de la protección de datos que forman parte del sistema" (Chicano, 2015).

"Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas." (Ramirez & Álvarez, 2003).

La Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial" (Lovos, s.f).

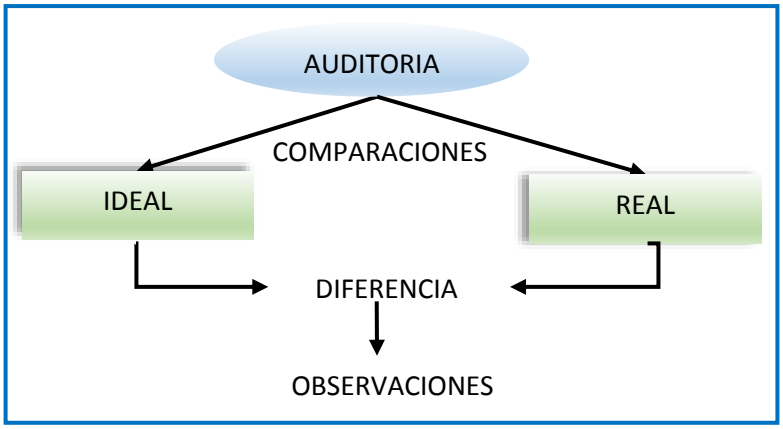


Figura N° 2 Esquema del concepto clásico de auditoria (Ramírez & Álvarez, 2003)

2.2.3 Activo Físico

"Los activos también son fundamentales para lograr los objetivos definidos por la organización y requieren de una especial protección: cualquier amenaza que pueda afectar a un activo puede poner en peligro la actividad de la organización y su servicio al cliente" (Chicano, 2015).

Un activo es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, que requiere protección. Posibles activos a identificar son: Activos de TIC (hardware, software, información), personal (empleados, invitados, usuarios de empresas de externalización), entorno (edificio, instalaciones), actividades (operaciones). (Areitio, 2008)

Un activo "es un elemento impreso o digital que contenga información, así como todo sistema - conformado por software, hardware y su documentación pertinente - que cree, maneje y procese información para una organización; también se puede incluir a la infraestructura tecnológica donde se desenvuelven dichos sistemas". (Tupia, 2010).

(ISO 27001:2013, 2015), Los activos son los recursos del Sistema de Seguridad de la Información, necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección. los activos se encuentran relacionados, directa o indirectamente, con las demás entidades según el siguiente esquema:

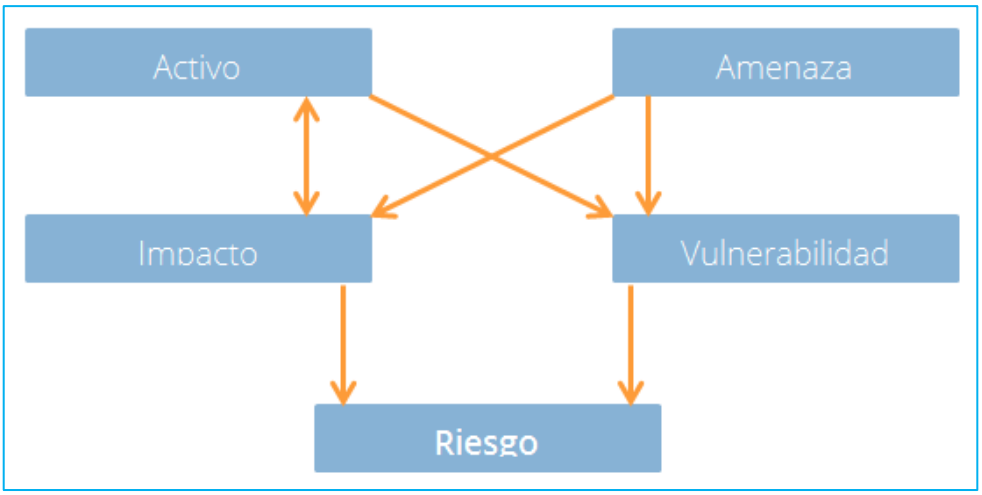


Figura N° 3 Relación de los activos (ISO Tools Excellence, 2013***)***

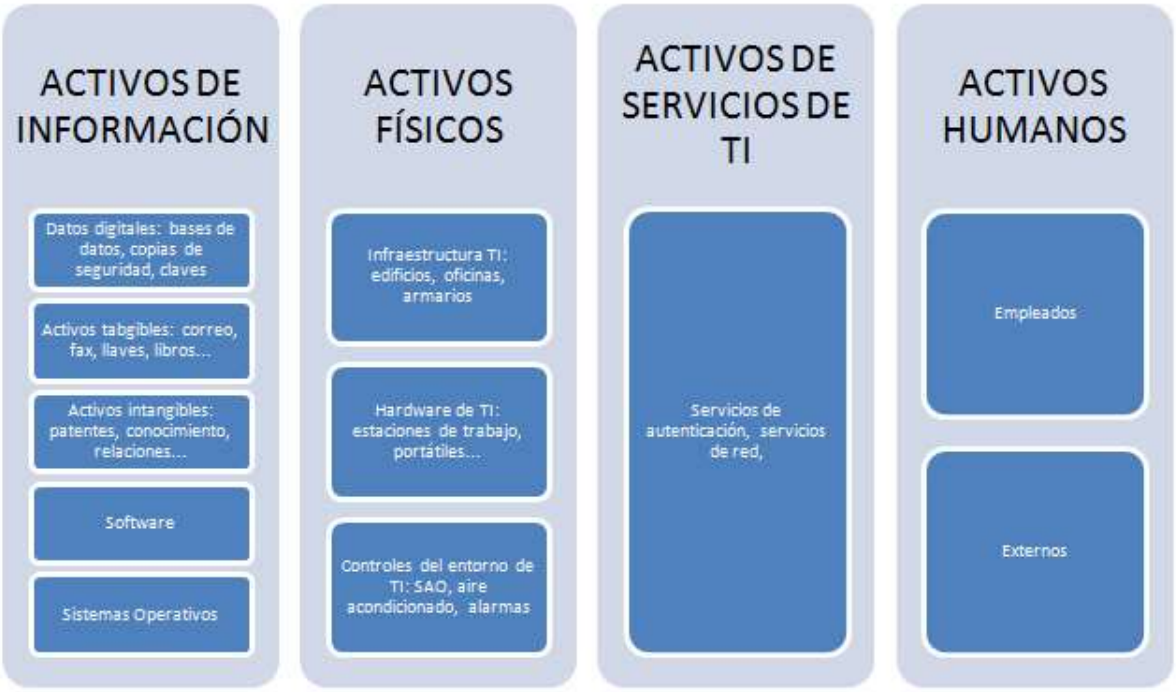


Figura N° 4 Clasificación general de los activos (ISOTools Excellence, 2013)

A. AMENAZA

Según (Costas, 2011) las amenazas a un sistema pueden provenir desde un hacker remoto que entra a un sistema, pasando por un programa descargado desde internet. La amenaza lógica es un software o código que de una forma u otra puede dañar un sistema informático, mientras que las amenazas físicas afectan a las instalaciones y/o hardware contenido en ella. Las amenazas pueden ser provocados por: personas, condiciones físico-ambientales y software.

Para (Piattini & Del peso, 2001), la amenaza es una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Ejemplos: inundación, incendio, robo de datos, sabotaje, agujeros públicos, falta de procedimiento de emergencia, divulgación de datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.

B. RIESGO

Para (Piattini & Del peso, 2001), el riesgo es "la probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad. Ejemplo: Jos datos estadísticos de cada evento de una base de datos de incidentes"

"El riesgo es la probabilidad de que una amenaza explote una vulnerabilidad. En los sistemas de la información se pueden asumir riesgos si el coste de la pérdida es bajo, pero existen entornos en los que el riesgo es muy alto y se han de implantar medidas para mitigarlo" (Cilleros, 2012)

Según (Nogueira, 2014), un riesgo "es el potencial de que exista una amenaza que pueda explotar una de las vulnerabilidades de los activos de la organización, produciéndole daño".

C. VULNERABILIDAD

Para (Piattini & Del peso, 2001) La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entone informático. Ejemplos: falta de control de acceso lógico, falta de control de versiones, inexistencia de un control de sopones magnéticos, falta de separación de entorno en el sistema, falta de cifrado en las telecomunicaciones, etc.

"Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas" (Seoane, Saiz, Fernández, & Fernández, 2010).

2.2.4 Impacto

(Aguilera, 2010), "un impacto es la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad o, dicho de otra manera, el daño causado".

(Areitio, 2008) "el impacto es la consecuencia de la materialización de una amenaza sobre un activo".

“Es la magnitud del daño que provoca un ataque exitoso. Dependiendo de los daños causados y los activos afectados, el impacto será mayor o menor” (Chicano, 2015)

2.2.5 Seguridad de la Información

La información es un recurso muy importante para las organizaciones, por lo que debe ser especialmente protegido. La seguridad de la información es la encargada de proteger esta amplia gama de amenazas, con el fin de garantizar la mejora continua de negocio, disminuir el daño que se pueda generar a la información e incrementar el retorno de las inversiones y las oportunidades de negocio. La información puede existir de muchas maneras. Puede estar impresa o en papel, se almacena de forma electrónica, se puede transmitir por un medio electrónico, en imágenes o en una conversación. Sea cual sea la forma en la que se encuentre la información o los medios mediante los que se distribuye o se almacena, siempre tiene que ser protegida de una forma adecuada (ISOTools Excellence, 2015).

Según la (NTP - ISO/IEC 17799 , 2007), La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información se caracteriza aquí como la preservación de:

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;
- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos;
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

2.2.6 Data Center

Según (Seoane, Saiz, Fernández, & Fernández, 2010), un data center es aquella ubicación en donde se concentran los recursos necesarios para el procesamiento de la información de una organización, dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas con toda la infraestructura necesaria en cuanto a Computadoras y Redes de Comunicaciones. También se le conoce con el nombre de Centro de Procesamiento de Datos (CDP) o simplemente su traducción del inglés, Centro de Datos (CD).

El Centro de Procesamiento de Datos (CPD) es un cuarto, espacio físico o ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. Se le conoce también como centro de cálculo en España, centro de cómputo en Iberoamérica, o centro de datos (data center). En dicho espacio se encuentran los equipos de una red, además de los servidores (Gómez, 2011)

Se denomina procesamiento de datos o CPD a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo (Iberoamérica) o centro de cálculo (España), o centro de datos por su equivalente en inglés data center. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, servidores y redes de comunicaciones. Un CPD, por tanto, es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento informático y en general electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. (Costas, 2011)

2.2.6.1 Áreas de Data Center

Según (Nogueira, 2014) un Data Center se compone de las siguientes áreas principales:

a) **Área de Distribución Principal (MDA)**

Área concentradora del sistema de cableado y que se encuentra dentro de la sala de cómputo. El MDA es una zona céntrica que alberga la conexión cruzada principal, así como Routers centrales y conmutadores para infraestructuras LAN y SAN. La MDA puede incluir una conexión cruzada horizontal (HC) para un área de distribución de equipos cercanos. La

norma requiere al menos un MDA y especifica la instalación de bastidores separados para fibra, UTP y cable coaxial en esta ubicación (Tongo, 2017).

Está ubicada en la parte central del Centro de Datos, contiene el Core o núcleo de las conexiones de red. En esta nace toda la operatividad de la red local y está conformada por los equipos principales de la red: Routers, módems y Switches. El Estándar establece a esta área como fundamental, puede haber más de una (en Centros de Datos grandes) y su implementación es obligatoria. (Dávila Cervantes & Ramírez Viteri, 2018).

b) Área de Distribución Horizontal (HDA)

Área que incluye los Switches de LAN/SAN y los del hardware como teclado, video y mouse para los equipos. En casos donde el centro de datos es pequeño, suele encontrarse incorporado al MDA. La HDA sirve como punto de distribución para el cableado horizontal y casas conexiones cruzadas y equipos activos de distribución de cable en el área de distribución de equipos. Al igual que la MDA, la norma específica la instalación de bastidores separados para fibra, UTP y cable coaxial en esta ubicación. También recomienda ubicar los interruptores y paneles de conexión para reducir al mínimo las longitudes de cordón de parcheo y facilitar la gestión de cables. La HDA se limita a 2.000 conexiones, y el número de HDAS es dependiente de la cantidad de cableado y el tamaño total del centro de datos (Tongo, 2017).

Esta área sirve para interconectar el cableado horizontal a los equipos que se encuentran en el Área de Distribución Principal. Es un punto de organización del cableado horizontal con conexiones directas y cruzadas entre los equipos de la red. El Estándar recomienda localizar esta área cerca los Switches y Patch panels de tal forma que se minimice la longitud de los Patch Cords y facilite su manejo y ordenamiento. (Dávila Cervantes & Ramírez Viteri, 2018).

c) Sala de Almacenamiento:

Área en la que se albergan las piezas de reposición y cableado.

d) Sala de Eléctrica/Mecánica:

Área que alberga los servicios primarios como son los circuitos de distribución.

e) **Sala de Telecomunicaciones:**

Área que mantiene lo equipos que abastecen los datos locales, video y voz necesario para las oficinas de soporte de las operaciones del centro de datos y otras áreas de trabajo. Subsistema donde se encuentra todas las áreas funcionales, así como las partes conformadas por el cable estructurado del centro de datos, cada una de estas áreas cumple con funciones ya definidas que aseguran una funcionabilidad óptima de toda la infraestructura. (Tongo, 2017)

f) **Centro de Operaciones:**

Centro de monitoreo del centro de datos. Son centros en el cual se encuentran los técnicos que monitorean el funcionamiento de las redes.

g) **Sala de Entrada:**

Sala que delimita con los equipos. Interface entre el proveedor de acceso y el cableado estructurado del centro de datos.

h) **Área de Distribución de los Equipos (EDA):**

Racks y gabinetes que contienen los módulos de computación y almacenamiento. Está conformada por un patrón alternativo que define el Estándar para crear pasillos "fríos" o "calientes" entre los racks y gabinetes que contienen los equipos, es decir, plantea una configuración que aplaque el calor de los dispositivos de red, de la manera más eficiente posible (Dávila Cervantes & Ramírez Viteri, 2018)

i) **Sala de Cómputo:**

Espacio donde se encuentran los equipos de datos, telecomunicaciones y cableado.

j) **Área de distribución zonal (ZDA):**

Área donde se albergan sólo los equipos pasivos. Se utiliza en caso de salas de cómputo amplias y debe tener una distancia determinada al HDA.

Esta área hace las veces de punto de organización que facilitará la reconfiguración de "equipos libres" tales como servidores o mainframes, es decir, es una zona donde se interconectan el Área de Distribución Horizontal y el Área de Distribución de Equipos. Esta área no contiene conexiones cruzadas o equipos activos de red. El Estándar define a esta área como opcional. (Dávila Cervantes & Ramírez Viteri, 2018).

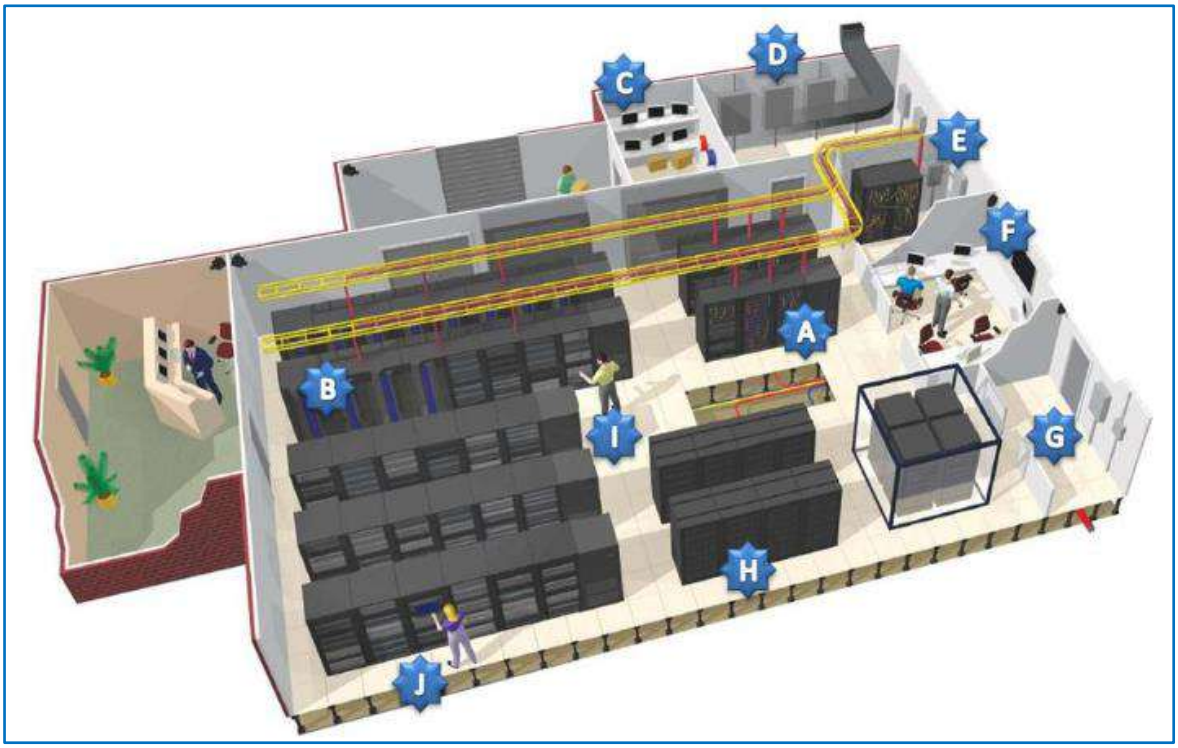


Figura N° 5 Distribución de áreas de un Centro de Datos (Tongo, 2017, pág. 38)

a) Área de Distribución Principal (MDA)

b) Área de Distribución Horizontal (HDA)

c) Cuarto de Almacenamiento

d) Cuarto de Máquinas Eléctricas/Mecánicas

e) Cuarto de Telecomunicaciones

f) Centro de Operaciones y Soporte

g) Cuarto de Entrada de Servicios

h) Área de Distribución de Equipos (EDA)

i) Cuarto de Computadores

j) Área de Distribución Local (ZDA)

2.2.6.2 Elementos Físicos de Data Center

Según (Nogueira, 2014), los elementos físicos de un Data Center son los siguientes:

Servidores Dedicados: Los servidores dedicados son aquellas computadoras designada para satisfacer determinadas necesidades de los sistemas o de los datos del negocio.

Cableado: El cableado es el elemento más importante de un Data Center, porque es a través de él que se transmite la energía que permitirá el funcionamiento de los distintos dispositivos tecnológicos, así como la comunicación entre diferentes medios.

Climatización: Es también un elemento sumamente importante pues, con el paso de los años, se ha buscado disminuir el tamaño de los dispositivos electrónicos, lo cual ha concentrado mayor potencia en un espacio más pequeño. Considerando que en una sala de cómputo se contarán con muchos dispositivos electrónicos ubicados cerca uno del otro, es importante ventilar la zona de manera que no se produzca una sobre carga por el calor, lo cual no solo afectaría a los equipos, sino que podría producir un accidente.

Energía: La electricidad es la parte más importante de un Data Center. Una interrupción en el fluido de energía, aunque sea por una fracción de segundo podría ocasionar una falla en el servicio y por lo tanto en el funcionamiento de la empresa. La energía es uno de los elementos que se necesita con disponibilidad del 100% para el funcionamiento de un Data Center, por lo cual se debe hacer todo lo posible para garantizar un suministro confiable e ininterrumpido de energía.

UPS: De las abreviaturas Uninterrupted Powers Supplies, es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía. Permite mantener el centro funcionando durante un período de tiempo determinado en caso de ocurrir un problema con el servicio de energía externa.

Seguridad: La seguridad es un elemento fundamental en un Data Center, no solo haciendo referencia a la seguridad de acceso físico que se debe tener, brindada por elementos como los sistemas biométricos de acceso a las áreas críticas o un sistema integrado de cámaras, sino también a controles ambientales que aseguren el buen estado de los equipos del centro de datos.

PUD: Se refiere al tablero para la distribución de energía confiable y de alto rendimiento. Las PUD se encuentran normalmente equipadas con sistemas de monitoreo de energía, los cuales permiten al usuario monitorear el consumo y la calidad de energía, así como gestionar y planear nuevas necesidades de energía.

Pasillos Fríos y Pasillos Calientes: La instalación de los sistemas en pasillos fríos y calientes responde a la necesidad de proporcionar una refrigeración más precisa y eficiente,

así como a la reducción de consumo energético. Todos los servidores y equipos de los Data Center están diseñados de manera que los ventiladores con los que se cuentan aspiren aire por la parte delantera y lo expulse por la parte trasera. La primera y la segunda fila de racks que contienen los servidores se colocan de manera que las partes frontales de ambas coincidan en un pasillo, por el cual se expulsará aire frío que enfriará la parte frontal de los servidores (pasillo frio). Si se incorpora otra fila, esta deberá ser colocada de forma que la parte trasera coincida en un pasillo con la parte trasera de la fila anterior, de manera que ambas líneas de rack expulsen el aire ya caliente al mismo pasillo (pasillo caliente)

2.2.6.3 Características del Data Center

Un Data Center es capaz de albergar recursos tecnológicos que permiten procesar una gran cantidad de información además de ser un ambiente acondicionado que contiene computadoras, equipos TIC, además de firewalls, Gateways VPN, Routers, servidores de banco de datos, de archivos, aplicaciones web y middleware en hardware físico o en plataformas consolidadas y virtualizadas, conectados en red y equipados con el software necesario para desarrollar el procesamiento de los datos (Date IT services, 2017).

Según (Nogueira, 2014), se detallan las características lógicas, físicas, electrónicas, ambientales y de diseño más importantes de un centro de datos.

a) Redundancia y Disponibilidad

La expectativa de un centro de datos es que cuente con una disponibilidad del 100% sin embargo, todos los centros de datos, sin importar cuan cuidadosamente hayan sido planificados, construidos y manejados, sufrirán de un período de tiempo de indisponibilidad, bien sea intencional o no intencional. La redundancia es una de las formas de reducir la indisponibilidad, pues no se cuenta con un solo elemento que provee servicios, por ejemplo, eléctricos, sino que se contará con alguna medida que permitirá que, de fallar un servicio, el otro pueda asumir el trabajo y así el negocio no sienta el efecto de la falla. (Nogueira, 2014).

Los Data Centers que están equipados con diversas instalaciones de telecomunicaciones deben ser capaces de continuar su función bajo condiciones catastróficas, puesto que de otra manera se interrumpirían los servicios de telecomunicaciones del mismo (Tongo, 2017).

b) Fiabilidad

La característica de fiabilidad está estrechamente relacionada con la redundancia y disponibilidad, pues un centro de datos debe ser diseñado de manera que se crea en el hecho de que no se aceptarán fallas durante todo el proceso de su funcionamiento. Uno de los mecanismos que permitirán confiar en el funcionamiento constante de un Data Center será la redundancia.

c) Manejabilidad

La manejabilidad nos indica la facilidad para el acceso, localización y reconfiguración de los elementos y características de los Data Center. Es necesario que, durante el diseño de éste, se busque como características la fiabilidad, flexibilidad y la integración de actualizaciones y modificaciones.

d) Espacio

Es uno de los elementos más valiosos para el diseño, pues se necesita asegurar que se cuenta con el espacio suficiente y que sea utilizado de la forma correcta. De la misma, para el cálculo del espacio se deberá considerar la posibilidad de la expansión del Data Center, considerando amplias áreas de espacio flexible libre para que se pueda reasignar a una función en particular.

e) Distribución

Es recomendable que se plantee la distribución de acuerdo a la realidad actual del centro de datos, así como a los objetivos de expansión de la empresa, permitiendo, por ejemplo, reasignar de forma fácil el espacio, administrar los cables para que no superen las distancias recomendadas de tendido, entre otros.

f) Administración de Cables

El significado de administración de los cables en el Data Center se refiere a la necesidad de tener un servicio de cableado confiable y flexible, de manera que puedan conectarse aplicaciones nuevas sencillamente. Para lograr un sistema cableado confiable, hay ciertos principios fundamentales:

- Se utilizan racks comunes en toda la distribución principal, así como en la horizontal, simplificando el montaje de rack.
- Se instalan administradores de cables vertical y horizontal

- Se instalan trayectorias para cables.
- Los cables UTP y coaxiales se separan de la fibra óptica para evitar aplastarla, de la misma forma, los cables eléctricos van en bandejas y la fibra en canales montados en bandejas.

g) Edificio

Los edificios en los que se establecerá el Data Center pueden ser de dos tipos de acuerdo a las necesidades y solvencia de la empresa. Muchas de ellas cuentan con el dinero adecuado para construir el centro de datos a su medida, con las características que necesita para manejar su negocio, mientras otras adecuan edificios para esta actividad.

La medida más adecuada para la construcción de un edificio para el Data Center, es que éste cuente con el espacio suficiente para colocar, de manera ordenada y definiendo en zonas, todos los equipos necesarios. De la misma forma, es importante definir su ubicación, que no solo van de la mano con consideraciones de tipo estratégico y económico, sino que debe precisar seguridad de la zona frente a riesgos impredecibles de la naturaleza, siendo la sala que alberga los equipos que precisan de mayores cuidados como la existencia de falso piso, falso techo, insonorización, climatización y suministro de energía.

h) Falso Piso

Constituido por baldosas independientes y movibles en madera o metal recubiertas por un revestimiento plástico que deben reposar sobre soportes de altura regulable que reposan en el pavimento. La altura del falso piso debe encontrarse entre los 0.05 y 0.075 m, pudiendo modificar la altura de acuerdo a las necesidades. El falso piso debe ser robusto e indeformable, resistente a la humedad, a la corrosión y a las cargas mal repartidas, debe asegurar el aislamiento de cargas estáticas y la protección de las personas.

Para el acceso y movimiento de materiales a la zona, los accesos a la sala deben estar equipados de una rampa de desnivel variable, rampa recubierta de goma estriada anti derrapante.

i) Ruido

Se debe considerar la posibilidad de altos niveles de ruido en el entorno de trabajo que puedan llegar a perturbar o producir molestias de salud a los trabajadores, por lo cual es preciso adoptar medidas oportunidad de insonorización. El objetivo de la insonorización es

eliminar al máximo las vibraciones sonoras en el interior del local del Data Center y al mismo tiempo evitar su propagación al exterior. Las medidas más comúnmente adoptadas son la insonorización del techo, suelo y paredes es con materiales como el corcho aglomerado, que reducirá las ondas que vienen o van al exterior, así como la insonorización de las máquinas por medio de carcasas de insonorización o bloques anti vibraciones.

j) Paredes

Las paredes deben ser pintadas con pintura ignífuga, cuya misión será retardar la acción destructora en caso de incendio, formando un aislamiento multicelular al reaccionar con la presencia de llamas. Los tipos de pintura ignífuga pueden ser:

- Extintoras: En contacto con el fuego emiten gases extintores
- Intumescente: Al entrar en contacto con las llamas se hincha, retardando el efecto de incendio.
- Mixtas: Realizarán la labor de las dos anteriores de forma simultánea, se hinchará desprendiendo gases extintores.

k) Ubicación de gabinetes

Los gabinetes deben ser ubicados de manera que el aire acondicionado oriente los flujos para realizar un intercambio adecuado de calor. Los patrones recomendables para la orientación son en bloques y conformando figuras geométricas, permitiendo extraer el calor generado por los equipos.

l) Temperatura

La temperatura es un factor importantísimo considerando que los equipos estarán en trabajo constante y por lo tanto generando calor constantemente. Los problemas principales derivados de la elevación de la temperatura son el apagado de los equipos por recalentamiento, así como el estrés en los componentes por cambios de temperatura. La temperatura promedio establecida es entre los 22°C y 24°C

m) Humedad

La humedad también es un factor importante pues puede producir deterioro en los equipos. Cuando los niveles de humedad son muy altos producirá corrosión, condensación y hongos, mientras que si es muy baja podría generar electricidad estática.

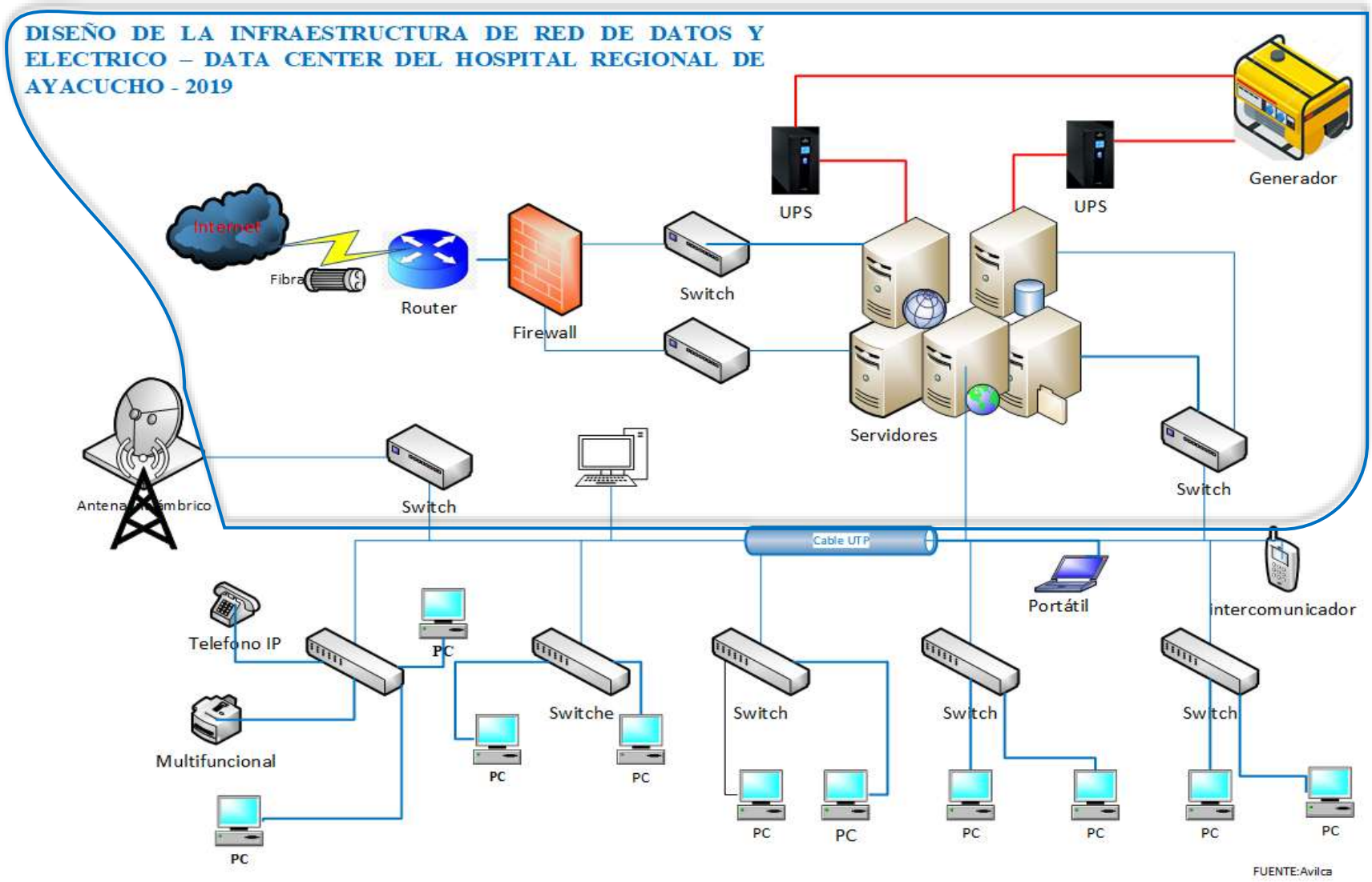


Figura N° 6 Diseño de red de datos y eléctrico del Data Center del Hospital Regional de Ayacucho -2019

2.2.7 Auditoría del Data Center

Los centros de datos son instalaciones industriales, muy especializadas, llena de equipos y sistemas muy complicados e interrelacionados. Los centros de datos se definen como tres infraestructuras: TI, electricidad y refrigeración. La infraestructura de TI se compone se equipos de TI con su respectivo software asociado (servidores, conmutadores de red y equipos de almacenamiento). La electricidad y la refrigeración son necesarios para que funcione la infraestructura de TI, le energía en bruta se transforma, convierte y se distribuye a los servidores. La refrigeración incluye refrigeración por líquido, por aire e inmersión, (ABB Review, 2012)

Los servicios de Auditoría garantizan la seguridad y continuidad del negocio. Es una parte estratégica de la actividad de la empresa y, por tanto, su seguridad y disponibilidad son esenciales. Un fallo en la infraestructura puede acarrear graves consecuencias. Para garantizar su operatividad, determinar su nivel de fiabilidad y seguridad, y conseguir su perfecto funcionamiento es indispensable realizar auditorías que permitan conocer con exactitud el "estado de salud" de la infraestructura del centro de datos, que identifiquen los posibles riesgos, las carencias o debilidades, así como los problemas de capacidad (Goal's, 2014).

(Goal's, 2014), Con las Auditorías es posible prevenir eventualidades posteriores no deseadas, definir las futuras líneas de actuación y eliminar riesgos de caídas del sistema. Estos últimos habrá que tenerlos muy presentes en las fases de diseño, ejecución y mantenimiento, ya que este tipo de averías pueden acarrear graves daños en el negocio. A través de una Auditoría se realizan estadísticas de utilización y capacidad, se identifican oportunidades para mejorar la disponibilidad y la eficiencia, se analiza la situación del Data Center en relación con la normativa aplicable y se definen las mejores prácticas en cuanto a:

Características de diseño y construcción, teniendo muy en cuenta la ubicación de la instalación, así como el alojamiento del equipamiento de TI, estándares...

- Sistema de refrigeración (climatización, pasillos fríos y calientes, flujos y pérdidas de aire)
- Sistema de energía.
- Sistema de cableado.
- Sistema de monitorización.

- Sistema de seguridad para prevenir y detectar incendios, inundaciones, control de accesos.
- Eficiencia energética.
- Procesos de operaciones

Una de las metodologías más recomendables para mejorar un Data Center es la de comenzar por realizar una auditoría de las instalaciones que incluya mediciones reales durante periodos de tiempo significativos. Toda esta información permite saber dónde se está realmente, con lo que es mucho más fácil tomar las decisiones correctas que permiten llegar al punto donde queremos estar (Cliatec, 2018).

2.2.8 Seguridad Física en Data Center

Según (Mtnet, 2018), La seguridad física de los data centers implica proteger la infraestructura crítica de amenazas externas o intrusiones que atenten contra las actividades de una empresa. Elementos de alto valor y sumamente importantes, tales como servidores, Switches y unidades de almacenamiento.

El mercado global de seguridad física para data centers se segmenta en cuatro niveles en base a las capas de seguridad:

1. Seguridad del perímetro
2. Seguridad de las instalaciones
3. Seguridad de la sala de ordenadores
4. Seguridad a nivel de racks

(Piattini & Del peso, 2001), señalan a continuación algunas fuentes que deben estar accesibles en todo Data Center al realizar una auditoría:

1. Políticas, normas y planes sobre seguridad.
2. Auditorías anteriores, generales y parciales, referentes a la seguridad física a cualquier otro tipo de auditoría que, de una u otra manera, esté relacionada con la seguridad física.
3. Contratos de seguros de proveedores y de mantenimiento.
4. Entrevistas con el personal de seguridad.

5. Actas e informes de técnicos y consultores (que diagnostiquen el estado físico del edificio, estado de operatividad de los sistemas de seguridad y alarma, agencias de seguridad que proporcionan a los vigilantes jurados, bomberos, etc).
6. Plan de contingencia y valoración de las pruebas.
7. Informes sobre accesos y visitas.
8. Informes sobre pruebas de evacuación ante diferentes tipos de amenaza: incendio, catástrofe natural, terrorismo, etc.
9. Informes sobre evacuaciones reales.
10. Política de personal. revisión de antecedentes personales y laborales, procedimientos de cancelación de contratos y despidos, rotación en el trabajo, planificación y distribución de tareas, contratos fijos y temporales.

2.2.9 Análisis de Riesgo

Para (Universidad Juárez Autónoma de Tabasco, 2006), "El análisis de riesgo puede ser considerado como, la identificación, el análisis, la evaluación, el control y la minimización de las pérdidas asociadas con eventos de riesgo, es una revisión constante y permanente debido a que se trata de un proceso continuo"

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados: 1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación 2. determinar a qué amenazas están expuestos aquellos activos 3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo 4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza 5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza (Consejo Superior de Administración Electrónica de España., 2012)

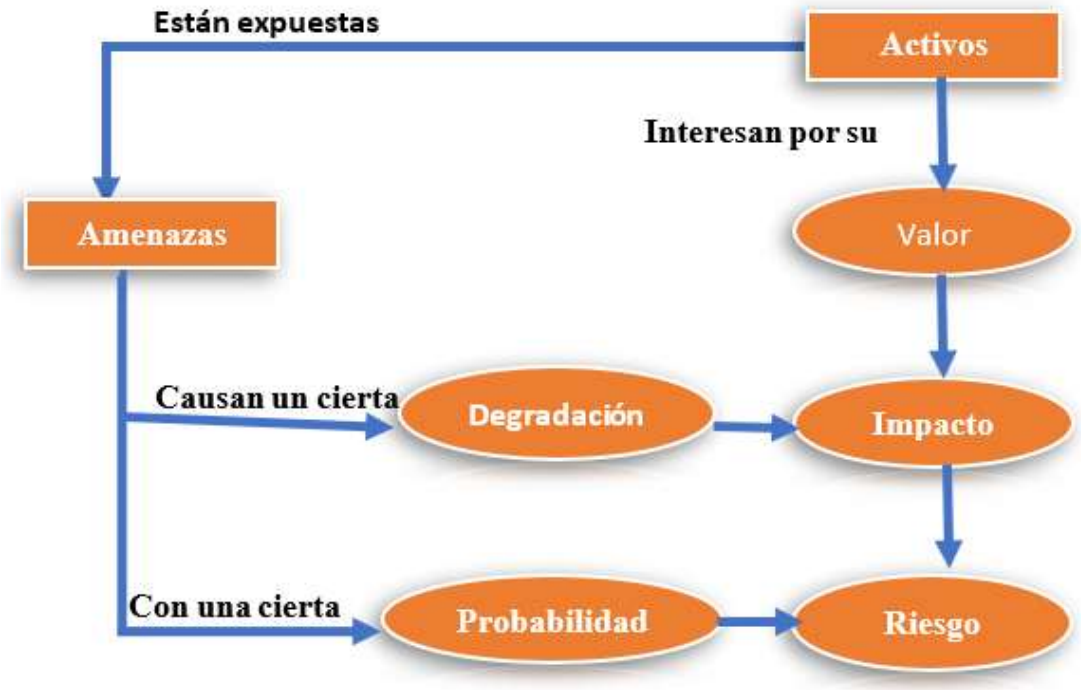


Figura N° 7 Elementos de análisis de riesgos potenciales. Magerit v.3 (2012)

El análisis de riesgos introduce un enfoque riguroso y consecuente para la investigación de los factores que contribuyen a los riesgos. En general implica la evaluación del impacto que una violación de la seguridad tendría en la empresa: señala los riesgos existentes. identificando las que afectan al sistema informático. y la determinación de la vulnerabilidad del sistema a dichas amenazas. Su objetivo es proporcionar una medida de las posibles amenazas y vulnerabilidades del sistema de manera que los medios de seguridad puedan ser seleccionados y distribuidos eficazmente para reducir al mínimo las posibles pérdidas. gestión de riesgos es un proceso separado que utiliza los resultados del análisis de riesgos para seleccionar e implantar medidas de seguridad (salvaguardas) adecuadas para controlar los riesgos identificados. (De Pablos, y otros, 2008)

Frente a estos riesgos potenciales analizados se puede:

- Aceptar el riesgo, dada en muchos casos su baja posibilidad de ocurrencia; ó
- Transferir el riesgo, contratando los correspondientes seguros (se debe tener en cuenta que a veces la información perdida es irremplazable) ó
- Evitar el riesgo.

Esto último conlleva la elaboración y puesta en marcha de un Plan de seguridad informática, cuyas medidas de carácter preventivo minimicen la probabilidad de ocurrencia de un nesgo.

Los métodos principales para el análisis y la gestión de riesgos de los SI son:

- MAGERIT, metodología pública española creada en 1996 el Ministerio de las Administraciones Públicas en colaboración con la empresa de tecnologías de la información Atos Origin y actualizada en su versión 2 en el año 2005.
- MARION, método francés nacido en 1985, que se actualiza CLUSIF (Asociación de empresas aseguradoras francesas)
- MELISA, procedente del entorno militar francés, que data de 1984.
- CRAMM, del CCVA (Central Computer and Telecommunications Agency) iniciado en 1985, que se usa preferentemente en la administración pública británica.
- OCTAVE, metodología del SEI (Software Engineering Institute) que desde un punto de vista organizativo y técnico analiza los riesgos y propone un plan de mitigación.
- OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad) metodología del ISECOM (INSTITUTE FOR SECURITI' AND OPEN METHODOLOGIES) propone evaluar la seguridad en redes con testeos de intrusión, a través de Hacking Ético

Según (Marulanda, 2014), De acuerdo con el estándar ISO/IEC 27001 el análisis del riesgo contempla lo siguiente:

A. Identificación de Activos

Según el (NTP - ISO/IEC 17799 , 2007), un activo de información es: "Algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (Asociación Española de Normalización, 2010)

El ISO 17799:2013 clasifica los activos de información en las categorías siguientes

- Activos de información
- Documentos del papel
- Activos de software

- Activos físicos
- Personal
- Imagen de la compañía y reputación
- Servicios

B. Tasación de Activos

La tasación de activos es un factor muy importante en la evaluación del riesgo. La tasación es la asignación apropiada en términos de la importancia que éste tenga para la empresa. Para ello se deberá aplicar una escala de valor a los activos y de esa manera poder relacionarlos apropiadamente.

La valoración se puede ver desde la perspectiva de la "necesidad de proteger" pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes. El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un es-quema de dependencias, acumulan el valor de los activos que se apoyan en ellos (Consejo Superior de Administración Electrónica de España., 2012).

Una práctica comúnmente utilizada al momento de realizar la tasación de activos es planteando la pregunta "¿Cómo una falla o perdida en un activo especifico afectan a la confidencialidad, la integridad y la disponibilidad?", para esto se debe establecer una escala del 1 al 5, en la cual 1 significa "muy poco" y 5 significa "muy alto" (Chamorro, 2013).

A continuación, en la tabla 1. se presenta un ejemplo de la tasación de activos según la escala de Likert.

Tabla N° 1
Tasación de activos

Valor	Significado
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Tasación de activos según la escala de Likert (Chamorro, 2013)

C. Identificación de Amenazas y Vulnerabilidades

"En esta definición, los autores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural" (como se cita en Marulanda, 2014, pág. 40).

plantea que una amenaza puede significar muchas cosas, depende del contexto en donde se le ubique. "Una amenaza es normalmente vista como un intento de hacer algo malo a alguien o a algo" (Thomas, 2010).

(Chamorro, 2013) indica que, en este punto, la empresa debe tomar decisiones importantes en relación con el análisis de las amenazas. La decisión sobre cuáles amenazas se descarta por su baja probabilidad de ocurrencia debe revisarse con detenimiento. Puede ocurrir que la amenaza con menor probabilidad de ocurrencia tenga las consecuencias más severas para la empresa.

D. Cálculo de Amenazas y vulnerabilidades.

(Chamorro, 2013) menciona que. una vez identificadas las amenazas y vulnerabilidades es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. El riesgo se define como: "La probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular"

E. Análisis del riesgo y su evaluación.

(ISOTools EXCELLENCE, s.f) indica que, se debe analizar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información, evaluando de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos. Además de riesgo en sí, es necesario analizar también sus consecuencias potenciales, que son muchas y de distinta gravedad: desde una simple dispersión de la información a la pérdida o robo de datos relevantes o confidenciales. Una posible metodología de evaluación de riesgos estaría compuesta de las siguientes fases:

1. Recogida y preparación de la información.
2. Identificación, clasificación y valoración los grupos de activos.
3. Identificación y clasificación de las amenazas.
4. Identificación y estimación de las vulnerabilidades.
5. Identificación y valoración de impactos: identificar, tipificar y valorar los impactos.

6. Evaluación y análisis del riesgo

2.2.10 LA AUDITORÍA

Para (Piattini & Del peso, 2001), Conceptualmente la Auditoría, toda y cualquier Auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones (Muñoz, 2012).

La auditoría es un examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, con frecuencia este término ha sido utilizado incorrectamente, ya que se ha considerado como una evaluación donde el fin es detectar errores y señalar fallas, pero el concepto de auditoría va más allá de la detección de errores, es un examen crítico donde el objetivo es evaluar la eficiencia y la eficacia de un área u organismo (Martínez, 2012).

2.2.10.1 La Auditoría Interna

Hernández (2010) manifiesta que la auditoría interna es una actividad que tiene por objetivo fundamental examinar y evaluar la adecuada y eficaz aplicación de los sistemas de control interno, velando por la preservación de la integridad del patrimonio de una entidad y la eficiencia de su gestión económica, proponiendo a la dirección las acciones correctivas pertinentes.

Es la revisión que realiza una profesional auditoría, cuya relación de trabajo es directa y subordinada a la institución se aplicará la misma, con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razonabilidad en la emisión de Sus resultados financieros. El objetivo final es contar con un dictamen interno sobre las actividades de toda la empresa, que permita diagnosticar la actuación

administrativa, operacional y funcional de empleados y funcionarios de las áreas que se auditan (Muñoz, 2012).

2.2.10.2 La Auditoría Externa

La auditoría externa es aquella que es realizada por una firma externa de profesionales con el propósito de examinar y evaluar cualquiera de los sistemas de información de una organización. Se trata de un procedimiento de uso común cuando se quiere comprobar que una empresa se maneja de forma honrosa. Se suele recurrir a las auditorías externas por ser agentes externos a la empresa y así poder tener un criterio más objetivo (González, 2015)

Es la revisión independiente que realiza un profesional de la Auditoría, con total libertad de criterio y sin ninguna influencia. el propósito de evaluar el desempeño de las actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como de la razonabilidad en la emisión de sus resultados financieros. la relación de trabajo del auditor es ajena a la institución donde se aplicará la auditoría y esto le permite emitir un dictamen libro e independiente. (Muñoz, 2012)

2.2.10.3 Auditoría Informática

Es la revisión técnica. especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes. así como a sus instalaciones, telecomunicaciones, mobiliario. equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática. el aprovechamiento de sus cursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa. (Muñoz, 2012)

Según (Piattini & Del peso, 2001) la auditoría informática también conocida como auditoría de sistemas de información es la revisión y la evaluación de los controles, de sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización, que participa en el procesamiento de la información, a fin de

que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

2.2.10.4 Seguridad Informática

(Seoane, Saiz, Fernández, & Fernández, 2010) indican que, tenemos que intentar lograr un nivel de seguridad razonable y estar preparados para que, cuando se produzcan los ataques, [os daños puedan ser evitados en unos porcentajes que se aproximen al ciento por cien o en caso contrario haber sido [o suficientemente precavidos para realizar las copias de seguridad y de esta manera volver a poner en funcionamiento [os sistemas en el menor tiempo posible.

La seguridad informática concierne a la protección de la información, que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema (Baldeón & Coronel, 2012)

Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables (Morlano, 2012).

2.2.11 Procedimientos De Auditoría

Según (Hevada, 2007), el proceso de la auditoría informática es un examen crítico, pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones, la revisión analítica a la suficiencia de controles establecidos en el ámbito informático, con la finalidad de disminuir los riesgos y garantizar la seguridad, confiabilidad y exactitud de la información.

De acuerdo a las actividades que serán evaluadas, se anotan los procedimientos a seguir para realizar la evaluación. En esta parte se especifican los pasos y demás instrucciones que servirán de guía para evaluar lo especificado; se pueden anotar tantos procedimientos como sean necesarios durante la evaluación. (Muñoz, 2012).

Para la presente investigación, se tomará en cuenta la "**metodología para realizar Auditoría de sistemas**" mencionada según (Muñoz, 2012) donde menciona de forma genérica, todas aquellas fases y pasos que se deben considerar en la planeación de la

evaluación. señala tres grandes apartados, las principales etapas que servirán de guía para la realización de una evaluación dentro del ambiente de sistemas computacionales.

2.3 METODOLOGÍA PARA REALIZAR AUDITORÍA

2.3.1 1ra Etapa: Planeación de la Auditoría

El primer paso para realizar una auditoría en sistemas computacionales es definir las actividades necesarias para su ejecución, lo cual se logrará mediante una adecuada planeación de estas; es decir, se deben identificar claramente las razones por las que se va a realizar la Auditoría y la determinación del objetivo de la misma, así como el diseño de los métodos, técnicas y procedimientos necesarios para llevarla a cabo y para preparar los documentos que servirán de apoyo para su ejecución, culminando con la elaboración documental de los planes. programas y presupuestos para dicha auditoría (Muñoz, 2012).

Su objetivo es obtener un conocimiento de la entidad u organización sobre cómo operan los sistemas de información que se han de incluir en la revisión y el ambiente de control en cuanto a las fuentes de información, evaluación de riesgos inherentes al control e identificación de controles claves, para definir el enfoque de Auditoría que se aplicará, determinar los procedimientos de Auditoría específicos a realizar, seleccionar al personal, determinar tiempo y costo y preparar los programas de auditoría respectivos (Navarro, 2005)

Según muñoz (2012), La etapa de planeación se divide en subetapas, se mencionan a continuación.

P.1 Identificar el Origen de la Auditoría

El primer paso formal para iniciar la planeación de una auditoría en el área de sistemas es identificar el origen de la auditoría; es decir, lo primero es saber por qué surge la necesidad o inquietud de realizar una auditoría. Para esto nos debemos preguntar ¿de dónde?, ¿por qué?, ¿quién? o para qué se requiere hacer la evaluación de algún aspecto de sistemas de la empresa. (Muñoz, 2012) menciona siete posibles causas. En esta investigación se tomará la causa posible tomando en cuenta los criterios y aspectos primordiales.

P.1.1 Por la carencia de planes de contingencia

El origen de esta auditoría de sistemas se debe a que no existe ningún plan de contingencia, ni un documento similar en donde se contemplen medidas preventivas o correctivas relacionadas con la seguridad de la información del área de sistemas. Es entonces

cuando, al conocer el nacimiento de la solicitud de una auditoría bajo este rubro, mucho ayudaría a valorar la necesidad de evaluar la implementación de los planes, programas y medidas preventivas de seguridad para el área de sistemas.

P.2 Realizar una visita preliminar al área que será evaluada.

Es recomendable, diríamos que casi imprescindible, que el auditor realice una visita preliminar al área de informática que será auditada, justo después de conocer el origen de la petición de auditoría, y antes de iniciarla formalmente; el propósito es que tenga un contacto inicial con el personal de dicha área y que observe cómo se encuentran distribuidos los sistemas, cuántos y cuáles son los equipos que están instalados en el centro de cómputo, cuáles son sus principales características, de qué tipo son las instalaciones, cuáles son medidas de seguridad Visibles que existen, y en Sí, que conozca la temática a la cual se enfrentará, de manera muy simple y de carácter tentativo

Dentro de esta visita preliminar, el auditor también aprovecha para establecer un contacto inicial con funcionarios, empleados y usuarios del área de sistemas; el propósito es que observe sus reacciones ante la realización de la auditoría, y que las posibles limitaciones y temores que influirán en la cooperación de dicho personal.

Otro aspecto que también se puede obtener de esta visita al área que será auditada, es que Se puede anticipar cuáles objetivos se pueden satisfacer con la auditoría, o por lo menos tratar de entender cuáles son las metas que se quieren alcanzar con la evaluación.

P.3 Establecer los objetivos de la Auditoría

El siguiente paso. después de haber identificado el origen de la Auditoría y haber realizado una visita preliminar al área que será auditada, es establecer lo más claramente posible el (los) objetivo(s) de la auditoría. ajustándose lo más posible a las necesidades de la evaluación. El propósito es establecer claramente lo que se busca con este tipo de trabajo.

En este paso se establecen los objetivos generales y específicos de la Auditoría para la investigación

P.4 Elaborar planes, programas y presupuestos para realizar la auditoría

Después de haber considerado todos los puntos antes señalados, el siguiente paso es realizar la planeación formal de la auditoría de sistemas, en la cual se concreten los planes, programas y presupuestos para dicha auditoría; es decir, se deben elaborar los documentos

que contemplen los planes formales para el desarrollo de la auditoría, los programas en donde Se delimiten perfectamente las etapas. eventos. y los tiempos de ejecución para cumplir con el objetivo, así como los presupuestos de la auditoría, documentos en donde Se deben asignar los Costos de los recursos que serán utilizados y el tiempo que serán utilizados para determinada actividad. A continuación, se señalan los aspectos que deben tener en cuenta en esta subetapa

Carátula de identificación del plan de auditoría. - Es la primera hoja del documento de planeación, en la cual se establecen lo más claramente posible Siguientes puntos:

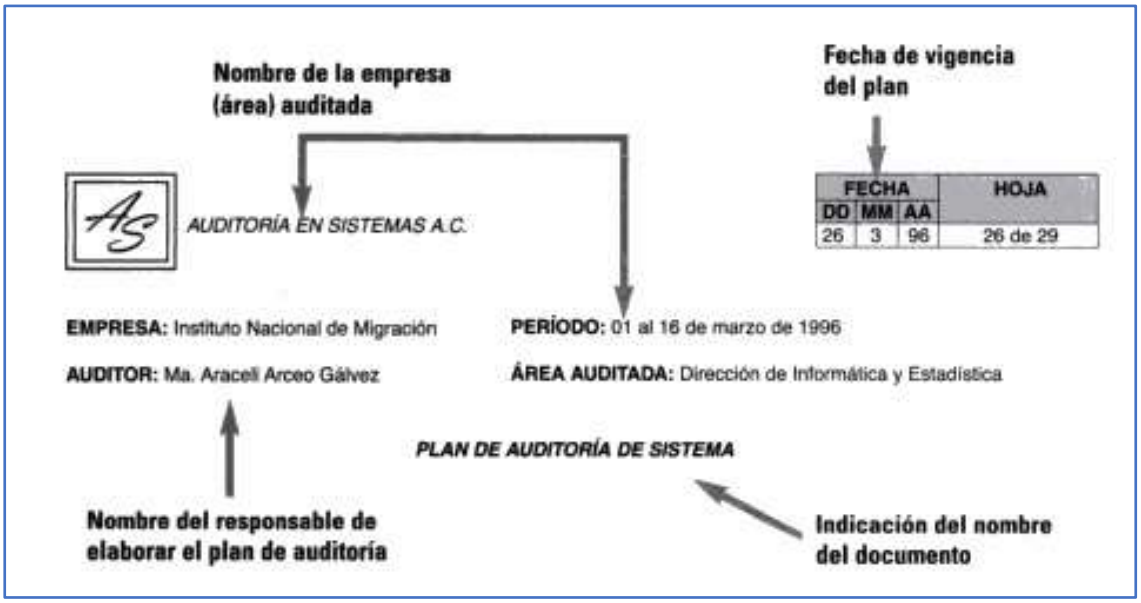


Figura N° 8 caratula de identificación de plan de auditoria (Muñoz, 2012)

P.5 Identificar y seleccionar los métodos. Procedimientos, instrumentos y herramientas necesarios para la Auditoría

El siguiente paso es determinar los documentos y medios con cuales se llevará a cabo la revisión a sistemas de la empresa, lo cual se logrará a través de la selección o diseño de métodos. procedimientos. herramientas e instrumentos necesarios: de acuerdo con lo indicado en los planes. presupuestos y programas establecidos para la auditoría. Para lograr esto, sugerimos Siguientes puntos:

- Establecer la guía de ponderación de los puntos que serán evaluados
- Seleccionar los métodos, procedimientos, herramientas e instrumentos de evaluación

P.6 Asignar los recursos y sistemas computacionales para la auditoría

Una vez definidos todos los aspectos señalados en las fases anteriores, el siguiente paso es asignar los recursos que serán utilizados para realizar la Auditoría, de acuerdo con los aspectos ya establecidos con anterioridad. Con la asignación de estos recursos sean humanos, informáticos, tecnológicos o cualesquiera otros que se establecido para la auditoría, es como se lleva a cabo la misma.

2.3.2 2da Etapa: Ejecución de Auditoría

Según (Loor & Espinoza, 2015), Esta etapa de la auditoría consiste en el desarrollo de los procedimientos contenidos en los programas de auditoría a través de técnicas de auditoría. Es la estructuración de un proceso uniforme para el desarrollo de las auditorías, en el cual las actividades están principalmente enfocadas a identificar riesgos de TI y evaluar la calidad de los controles para la gestión de los riesgos.

Para (Muñoz, 2012), El siguiente paso después de la planeación de la auditoría es su ejecución, la cual estará determinada por las características concretas, los puntos y requerimientos que se estimaron en la etapa de planeación. Debido a que esta etapa es de realización especial, de acuerdo con la planeación de la auditoría, en este inciso sólo se indican sus puntos más importantes, en la inteligencia de que se aplicará verdaderamente de acuerdo a las características específicas de la auditoría que se trate. Los principales puntos son los siguientes:

E.1 Realizar las acciones programadas para la auditoría

De acuerdo con el programa de Auditoría, cada auditor tiene que realizar las actividades que le corresponden conforme fueron diseñadas, en la cronología que le fue asignada a cada una, y de acuerdo con los tiempos y recursos que le corresponde utilizar; el propósito es ejecutar los eventos programados y el objetico de la Auditoría.

E.2 Aplicar los instrumentos y herramientas para la auditoría

Aquí lo importante es que, conforme a la guía de auditoría, se tienen que utilizar, uno a uno, los instrumentos y herramientas elegidos para llevar cabo la evaluación. ya se mediante la recopilación y análisis de la información, la observación. las pruebas y simulaciones de los sistemas. o mediante cualquier otro instrumento de los que se diseñaron previamente para esta revisión

E.3 Integrar el legajo de papeles de trabajo de la Auditoría

El auditor tiene la obligación de conservar en el llamado legajo de papeles de la auditoría cada uno de los instrumentos aplicados en la evaluación, con el propósito de sustentar. llegado el caso. las observaciones reportadas (Whitten, 2008)

HALLAZGOS DE AUDITORÍA

Los hallazgos en la auditoría, se definen como asuntos que llaman la atención del auditor y que en su opinión, deben comunicarse a la entidad, ya que representan deficiencias importantes que podrían afectar en forma negativa, su capacidad para registrar, procesar, resumir y reportar información confiable y consistente, en relación con las aseveraciones efectuadas por la administración (Whitten, 2008)

El término hallazgo se refiere a debilidades en el control realizado, detectadas por el Auditor. Por lo tanto, abarca los hechos y las informaciones obtenidas que merecen ser comunicados a los encargados de la entidad auditada y a otras personas interesadas.

ELEMENTOS DEL HALLAZGO DE AUDITORÍA

Según (Piattini & Del peso, 2001), desarrollar en forma completa todos los elementos del hallazgo en una auditoría, no siempre podría ser posible. Por lo tanto, el auditor debe utilizar su buen juicio y criterio profesional para decidir cómo informar determinada debilidad importante identificada en el control interno. La extensión mínima de cada hallazgo de auditoría dependerá de cómo éste debe ser informado, aunque por lo menos, el auditor debe identificar los siguientes elementos:

- **Condición:** Se refiere a la situación actual encontrada por el auditor al examinar un área, actividad, función u operación, entendida como "lo que es".
- **Criterio:** Comprende la concepción de "lo que debe ser ", con lo cual el auditor mide la condición del hecho o situación.
- **Efecto:** Es el resultado adverso o potencial de la condición encontrada, generalmente representa la pérdida en términos monetarios originados por el incumplimiento para el logro de la meta, fines y objetivos institucionales.
- **Causa:** Es la razón básica (o las razones) por lo cual ocurrió la condición, o también el motivo del incumplimiento del criterio de la norma. Su identificación requiere de la habilidad y el buen juicio del auditor y, es indispensable para el desarrollo de una recomendación constructiva que prevenga la recurrencia de la condición.

Evidencias De Auditoría

La evidencia de auditoría es el conjunto de hechos comprobados, suficientes, competentes y pertinentes (relevantes) que sustentan las conclusiones de auditoría. Las evidencias de auditoría constituyen los elementos de prueba que obtiene el auditor sobre los hechos que examina y cuando éstas son suficientes y competentes, constituyen el respaldo del examen que sustenta el contenido de la auditoría (Govindan, 2007)

Indica la obligatoriedad de obtener evidencia suficiente, competente y pertinente para sustentar los hallazgos de auditoría.

2.3.3 3ra Etapa: Dictamen de la Auditoría

Según (Muñoz, 2012), "el último paso de la metodología que hemos estudiado es emitir el dictamen, el cual es el resultado final de la auditoría de sistemas computacionales". Para ello presentamos los siguientes puntos:

D.1 Analizar la información y elaborar un informe de situaciones detectadas.

Después de analizar los informes anteriores (el borrador inicial comentado). el auditor debe elaborar, de manera formal, el informe de las desviaciones encontradas, especificándolas por área por servicio o por cualquier otro formato de presentación, de manera clara y precisa. También deberá presentar las desviaciones conforme a la costumbre de la empresa; ya sea importancia, por orden cronológico, por secuencia de operaciones o por cualquier otro criterio, siempre y cuando éste sea igual en toda la elaboración del informe.

D.2 Elaborar el dictamen final.

El auditor debe terminar de elaborar el informe de auditoría de sistemas y complementarlo con el dictamen final (opinión del auditor), y después presentarlo a los directivos del área de sistemas auditada para que conozcan la situación actual de dicha área, antes de presentarlo al responsable de la empresa.

D.3 Presentar el informe de auditoría.

Es de suma importancia destacar que el dictamen y el informe final de la auditoría deben ser elaborados perfectamente y no deben tener error alguno. También deben contener, de la manera más clara y concreta, las desviaciones detectadas en la evaluación.

2.4 COBIT 5

Para (ISACA, 2012), COBIT 5 es un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Ayuda a las empresas a crear un valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5.0 permite a las TI ser gobernadas y gestionadas de un modo holístico, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI.

COBIT 5.0 se basa en cinco principios para el gobierno y la gestión de las TI empresariales

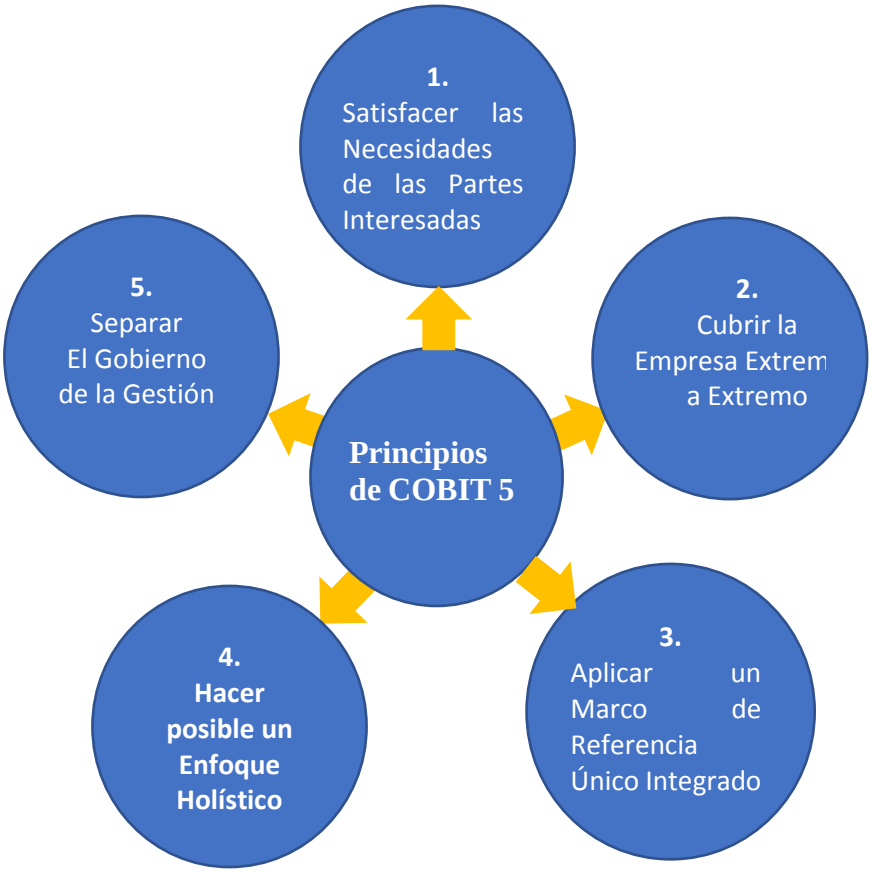


Figura N° 9 Principios de COBIT 5.0 (ISACA, 2012)

A. Satisfacer las necesidades de las partes interesadas

Según (ISACA, 2012), la empresa existe para crear valor entre las partes interesadas manteniendo el equilibrio entre la realización de los beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5.0 provee los procesos necesarios para permitir la creación de valor del negocio mediante el uso de TI. Las empresas pueden personalizar COBIT 5.0 adaptándolo a su propia realidad mediante la cascada de metas, traduciendo metas corporativas de alto nivel a metas más específicas relacionadas a TI. 22

B. Cubrir la empresa extrema a extremo

Según (ISACA, 2012), este principio cubre todas las funciones y procesos dentro de la empresa; COBIT 5.0 no se enfoca sólo en la función de TI, sino trata a la información y las tecnologías como activo que deben ser tratados como cualquier otro activo por toda la empresa. Considera que los Catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin.

C. Aplicar un marco de referencia único integrado

Según (ISACA, 2012), existen muchos estándares y buenas prácticas relacionadas a TI, COBIT 5.0 se alinea a alto nivel con otros estándares y marco de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y gestión de las TI de la empresa.

D. Hacer posible un enfoque holístico

Según (ISACA, 2012), un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico. COBIT 5.0 define un conjunto de Catalizadores para apoyar la implementación de un sistema de gobierno y gestión global de las TI de la empresa. Los Catalizadores se definen como cualquier cosa que ayuden a conseguir las metas de la empresa.

E. Separar el gobierno de la gestión

Para (ISACA, 2012), COBIT 5.0 estable una clara diferencia entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven diferentes propósitos.

2.4.1 CICLO DE VIDA DE COBIT 5.0

El ciclo de vida de COBIT 5.0 proporciona a las empresas una manera de usar COBIT para solucionar la complejidad y el desafío que aparece durante la implementación. Hay tres componentes del ciclo de vida interrelacionados: a) ciclo de vida de mejora continua, b) habilitación de cambio y c) gestión del programa. Este ciclo de vida cuenta con siete fases (ISACA, 2012).

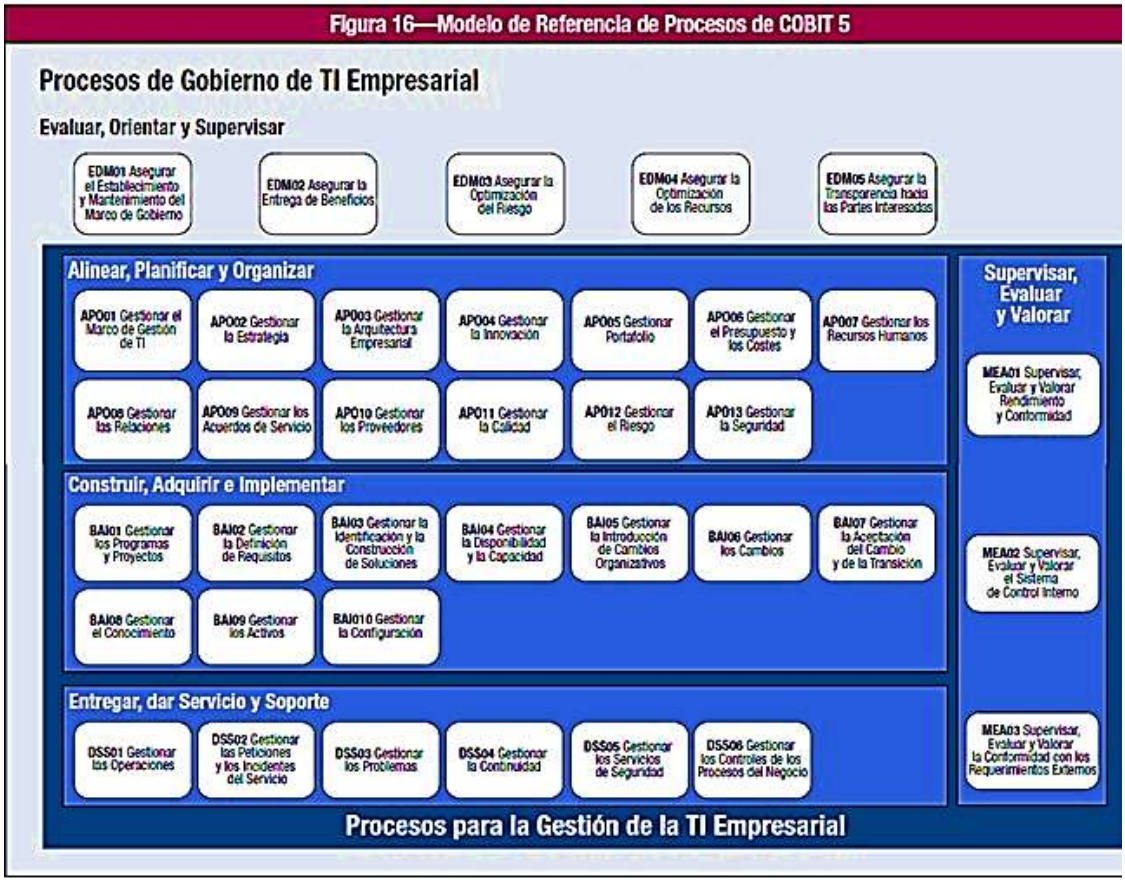


Figura N° 11 Modelo de procesos COBIT 5.0 (ISACA, 2012)

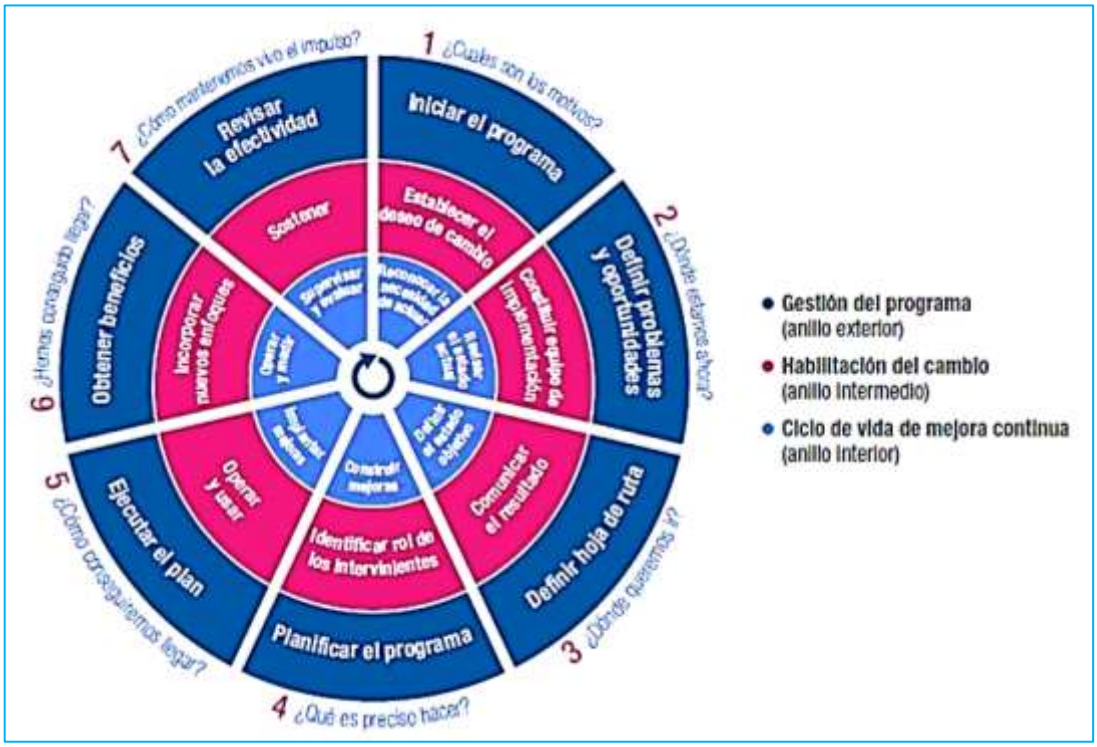


Figura N° 10 Ciclo de vida de implementación de COBIT 5.0 (ISACA, 2012)

2.4.2 Modelo De Referencia de Procesos COBIT 5.0

Según (ISACA, 2012), el modelo de referencia de procesos COBIT subdivide los procesos de gobierno y de gestión de TI en dos principales áreas de actividad; gobierno y gestión y a su vez dividido en dominios de procesos. El dominio de gobierno tiene cinco procesos; en cada uno de ellos se define prácticas de Evaluación, Dirección y Supervisión (EDM, sigla en inglés) y el dominio de gestión tiene 4 procesos alineados con las áreas de Responsabilidad de planificación, Construcción, Ejecución y supervisión (PBRM, sigla en inglés).

2.4.3 NTP-ISO/IEC 17799

Según (ISO/IEC - INDECOPI, 2014), La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de abril a junio del 2014, utilizando como antecedente a la norma ISO/IEC 27001:2013 Información Tecnología.

El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias -CNB-, con fecha 2014-08-19, el PNTP-ISO/IEC 27001:2014, para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2014-10-18. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 2ª Edición, el 01 de diciembre de 2014.

Esta Norma Técnica Peruana reemplaza a la NTP-ISO/IEC 27001:2008 (revisada el 2013) y es una adopción de la norma ISO/IEC 27001:2013 y de la ISO/IEC 27001:2013/COR 1 . La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada en concordancia a las Guías Peruanas GP 001:1995 y GP 002:1995.

La Norma está estructurado por 11 cláusulas de control de seguridad y un total de 39 categorías principales de seguridad y una cláusula introductoria que trata sobre evaluación y tratamiento de riesgos.

l. Política de seguridad

a. Política de seguridad de la información.

2. Aspectos organizativos para la seguridad

a. Organización interna.

b. Seguridad en los accesos de terceras partes.

3. Clasificación y control de activos

a. Responsabilidad sobre los activos.

b. Clasificación de la información.

4. Seguridad en Recursos Humanos

a. Seguridad antes del empleo.

b. Durante el empleo.

c. Finalización o cambio del empleo.

5. Seguridad física y ambiental

a. Áreas seguras.

b. Seguridad de los equipos.

6. Gestión de comunicaciones y operaciones

a. Procedimientos y responsabilidades de operación.

b. Gestión de servicios externos.

c. Planificación y aceptación del sistema.

d. Protección contra software malicioso.

e. Gestión de respaldo y recuperación.

f. Gestión de seguridad en redes.

g. Utilización de los medios de información.

h. Intercambio de información.

i. Servicios de correo electrónico.

j. Monitoreo.

7. Control de accesos

a. Requisitos de negocio para el control de accesos.

b. Gestión de acceso de usuarios.

c. Responsabilidades de los usuarios.

d. Control de acceso a la red.

e. Control de acceso al sistema operativo.

f. Control de acceso a las aplicaciones y la información.

g. Informática móvil y teletrabajo.

8. Adquisición, desarrollo y mantenimiento de sistemas

a. Requisitos de seguridad de los sistemas.

b. Seguridad de las aplicaciones del sistema.

c. Controles criptográficos.

d. Seguridad de los archivos del sistema.

e. Seguridad en los procesos de desarrollo y soporte:

f. Gestión de la vulnerabilidad técnica

9. Gestión de incidentes en la Seguridad de Información

a. Reportando eventos y debilidades de la seguridad de información

b. Gestión de las mejoras e incidentes en la seguridad de información

10. Gestión de continuidad del negocio

a. Aspectos de la gestión de continuidad del negocio

11. Cumplimiento

a. Cumplimiento con los requisitos legales.

b. Revisiones de la política de seguridad y de la conformidad técnica.

c. Consideraciones sobre la Auditoría de sistemas

2.4.4 POBLACIÓN

Según (Córdoba, 2003), se denomina población o universo a la totalidad de personas u objetos que tiene características medibles de naturaleza cualitativa o cuantitativa, la característica contable es una característica contable cuyo valor numérico o no numérico es una observación, en otras palabras, la población se puede definir como un conjunto de valores posibles de la variable.

define a la población como un universo de estudio de la investigación, y sobre el cual se puede generalizar los resultados, constituidos por características que le permita distinguir los sujetos unos de otros (Chavez, 2007).

2.4.5 MUESTRA

Según (Córdoba, 2003), la muestra es un subconjunto de la población, que posee las mismas características de la población y que a partir de las muestras se puede inferir los resultados hacia la población.

Para (Tamayo & Tamayo, 1997) la muestra es un grupo de individuos que se toma de la población con un fin de estudio estadístico.

(Ary, 1996). señala que "…si la población posee pequeñas dimensiones, deben ser seleccionados en su totalidad, para así reducir el error en la muestra…". Tomando como fundamento esta definición, podemos determinar que la muestra es aquella que representa en su totalidad los individuos que permiten obtener información sobre el tema a investigar.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 TIPO Y NIVEL DE INVESTIGACIÓN

A TIPO DE INVESTIGACIÓN

Según (Supo, s.f), son estudios observacionales en los cuales ningún acto del investigador modifica los resultados de la medición, incluso si es el propio investigador quien realizo las mediciones; de esta manera, los datos encontrados y la información consignada refleja el estado natural de las unidades de estudio.

Según (Hernández, Fernández, & Baptista, 2010), define la investigación observacional como aquella "investigación que se sustenta en el uso de técnicas que permiten al investigador adquirir información por medio de la observación directa y el registro de fenómenos, pero sin ejercer ninguna intervención".

Según (Supo, s.f), los estudios prospectivos son aquellos que se realizan con datos que provienen de mediciones controladas, hechas por el propio investigador, de manera que se asegure contar con datos que provienes de mediciones controladas, donde los sesgos de medición han sido controlados.

Según (Hernández, Fernández, & Baptista, 2010), el tipo de investigación transaccional o transversal recolecta datos en un solo momento, en un tiempo único. Su propósito es describir variables, y analizar su incidencia e interrelación en un momento dado.

Según Dr. (Supo, s.f), Los estudios con una sola medición son los denominados transversales, son aquellos estudios donde todas sus variables son medidas en una sola ocasión, independientemente del tiempo que nos tome realizar las mediciones de todos los elementos que conformen el grupo de estudio. Esta clasificación nada tiene que ver con la duración del estudio.

(Bernal Torres, 2010), "La investigación descriptiva se soporta principalmente en técnicas como la encuesta, la entrevista, la observación y la revisión documental".

Según (Supo, s.f), en el tipo de investigación descriptivo el análisis estadístico, es univariado porque solo describe o estima parámetros en la población de estudio a partir de una muestra.

En la presente investigación se desarrollará una auditoría a la seguridad física del Data Center del Hospital Regional de Ayacucho; donde no pretendemos manipular las variables para tratar de producir resultados, en su lugar, observamos y comparamos los sujetos con un grupo de control, la planificación para la toma de datos son registros de un inventariado hecho por el propio investigador, el número de veces en que se mide el variable de interés es en un solo momento, usando el marco control COBIT 5.0 y NTP-ISO/IEC 17799 y en número de variable es único. Por estas consideraciones el tipo de investigación es observacional, prospectivo, transversal y descriptivo.

B NIVEL DE INVESTIGACIÓN

Según (Hernández, Fernández, & Baptista, 2010), Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Describe tendencias de un grupo o población.

Según Dr. (Supo, s.f), el estudio de nivel descriptivo, tiene en su enunciado a la variable de estudio, que en este caso será única, otras variables participantes se denominan variables de caracterización y no aparecen en el enunciado del estudio, puesto que no habrá relación entre variables, pero si aparecen en el cuadro de operacionalización.

(Bernal Torres, 2010), En tales estudios se muestran, narran, reseñan o identifican hechos, situaciones, rasgos, características de un objeto de estudio, o se diseñan productos, modelos, prototipos, guías, etcétera, pero no se dan explicaciones o razones de las situaciones, los hechos, los fenómenos. La investigación descriptiva se soporta principalmente en técnicas como la encuesta, la entrevista, la observación y la revisión documental.

En la presente investigación se diseñará procedimientos para la auditoría en la seguridad física del Data Center del Hospital Regional de Ayacucho, el cual ayudará al auditor en la revisión y evaluación de los controles de seguridad, usando el marco de control COBIT 5.0, la Norma Técnica Peruana NTP-ISO/IEC 17799:2007. Por estas consideraciones el nivel de la investigación es descriptivo.

C DISEÑO DE LA INVESTIGACIÓN

Según (Hernández, Fernández, & Baptista, 2010), Podría definirse como la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios donde no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para posteriormente analizarlos.

Los diseños de investigación transeccional o transversal recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado. Es como tomar una fotografía de algo que sucede (Hernández et al. 2010).

En la presente investigación observamos, generamos los datos en un momento determinado de la investigación, medimos dichos valores en un único momento y sometemos a medidas a través de técnicas para concluir. En tal sentido, la presente investigación de acuerdo con los objetivos planteados, pertenece a investigación no experimental.

3.2 POBLACIÓN Y MUESTRA

POBLACIÓN. - La población de estudio analizada, estuvo compuesta por todos los procesos de control de la seguridad Física del Data Center del Hospital Regional de Ayacucho en el año 2019.

MUESTRA. - (Areitio, 2008) señala que "…si la población posee pequeñas dimensiones, deben ser seleccionados en su totalidad, para así reducir el error en la muestra…". En efecto se tomó una muestra por conveniencia conformado por todos los activos físicos del Data Center del Hospital Regional de Ayacucho en el año 2019.

3.3 VARIABLES E INDICADORES

DEFINICIÓN CONCEPTUAL DE LAS VARIABLES

VARIABLE DE INTERÉS

Seguridad de física. - la Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

En un Data center: Se refiere a los controles y mecanismos de seguridad dentro y alrededor, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos

INDICADORES DE LA VARIABLE DE INTERÉS

Activo Físico. – son aquellos recursos con las que cuenta una organización, es la base para la gestión de riesgos de seguridad de la información y para determinar los niveles de protección requeridos. se define como todo objeto o bien material que posee una persona natural o jurídica, tales como maquinarias, equipos, edificios, muebles, vehículos, materias primas, productos en proceso, herramientas, etc.

Amenaza. -la amenaza es una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Una amenaza es normalmente vista como un intento de hacer algo malo a alguien o a algo

Riesgo. - Un riesgo es lo posibilidad de que se produzca un impacto negativo para lo empresa aprovechando alguno de sus vulnerabilidades.

Es la probabilidad latente de que ocurra un hecho que produzca ciertos efectos, la combinación de la probabilidad de la ocurrencia de un evento y la magnitud del impacto que puede causar, así mismo es la incertidumbre frente a la ocurrencia de eventos y situaciones que afecten los beneficios de una actividad

Criterios de Seguridad Física. – Se plasma en una serie de normas, reglamentos y protocolos a seguir donde se definen las distintas medidas a tomar para proteger la seguridad física, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar el funcionamiento correcto.

DEFINICIÓN OPERACIONAL DE LAS VARIABLES

VARIABLE X

X: Seguridad Física

VARIABLES DESCRIPTIVAS

X1: Activo Físico

X2: Amenaza

X3: Riesgo

X3: Criterios de Seguridad Física

OPERACIONALIZACIÓN DE LAS VARIABLES

Se muestra en el Anexo A.

3.4 TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

3.4.1 TÉCNICAS

(Tamayo y Tamayo, 2004), La técnica viene a ser un conjunto de mecanismos, medios y sistemas de dirigir, recolectar, conservar, reelaborar y transmitir datos. Es también un sistema de principios y normas que auxilian para aplicar los métodos, pero realizan un valor distinto. Las técnicas de investigación se justifican por su utilidad, que se traduce en la optimización de los esfuerzos, la mejor administración de los recursos y la comunicación de los resultados.

OBSERVACION. - Se define como una técnica de recolección de datos que permite acumular y sistematizar información sobre un hecho o fenómeno social que tiene relación con el problema que motiva la investigación. En la aplicación de esta técnica, el investigador registra lo observado, mas no interroga a los individuos involucrados en el hecho o fenómeno social; es decir, no hace preguntas, orales o escrita, que le permitan obtener los datos necesarios para el estudio del problema (Chávez de Paz, s.f)

LA ENTREVISTA. - La entrevista, conjuntamente con el cuestionario son técnicas de la encuesta. Este es un método de investigación social que sigue los mismos pasos de la investigación científica; sólo que en su fase de recolección de datos, éstos se obtiene mediante un conjunto de preguntas, orales o escritos, que se les hace a las personas involucradas en el problema motivo de estudio (Chávez de Paz, s.f).

EL CUESTIONARIO. - El cuestionario es una técnica de recolección de datos y está conformado por un conjunto de preguntas escritas que el investigador administra o aplica a las personas o unidades de análisis, a fin de obtener la información empírica necesaria para determinar los valores o respuestas de las variables es motivo de estudio (Chávez de Paz, s.f).

3.4.2 INSTRUMENTOS

(Calderero hernandez & Bernardo Carrasco, 2000), consideran que los instrumentos es un recurso del que puede valerse el investigador para acercarse a los fenómenos y extraer de ellos información. Dentro de cada instrumento pueden distinguirse dos aspectos diferentes: una forma y un contenido. La forma del instrumento se refiere al tipo de aproximación que establecemos con lo empírico, a las técnicas que utilizamos para esta tarea. En cuanto al contenido, éste queda expresado en la especificación de los datos concretos que necesitamos conseguir; se realiza, por tanto, en una serie de ítems que no son otra cosa que los indicadores bajo la forma de preguntas, de elementos a observar, etc.

Se ha diseñado el instrumento "**cuestionario de encuestas**", para el registro de preguntas realizadas al personal del área, y que permita construir la matriz para realizar la Auditoría de la seguridad física, presentado en el Anexo B.

Se ha diseñado el instrumento "**cuestionario de entrevista**", para hacer las entrevistas al personal encargado del Data Center del Hospital Regional de Ayacucho, y que permita construir la matriz para realizar la Auditoría de la seguridad física, presentado en el Anexo C.

3.4.2.1 VALIDEZ DEL INSTRUMENTO

(Hurtado & Toro, 2005) Definen que "la validez es el grado en que la medición representa al concepto medido", es un concepto del cual pueden tenerse diferentes tipos de evidencias relacionadas con el contenido, criterio y con el constructo". La validez de contenido se refiere al grado en que un instrumento refleja un dominio específico de contenido de lo que se mide.

La validez de criterio establece la validez de un instrumento de medición comparándola con algún criterio externo, que es un estándar con el que se juzga la validez del instrumento, considerándose que entre más se relacionen los resultados del instrumento de medición con el criterio, la validez del criterio será mayor.

3.4.2.2 INSTRUMENTOS DE APOYO

Ficha Bibliográfica. - La ficha bibliográfica es un instrumento de investigación documental y de campo en el que se anotan, atendiendo a un orden y forma preestablecidos, los datos de

una obra (libro, folleto, artículo de revista, etc.) ya publicada, para poderla identificar y distinguir de otras o de sus diferentes ediciones.

Reporte de Página Electrónica. - El internet es red de redes de comunicación que ayuda en la búsqueda de información para la investigación u otro fin, en esta investigación también se utiliza los sitos confiables para el desarrollo de la investigación.

Referencia. - Es un instrumento para hacer cita de alguna obra donde él investigador puede encontrar mayor información de la que se presenta.

Checklist. - La lista de chequeo, como herramienta metodológica está compuesta por una serie de ítems, factores, propiedades, aspectos, componentes, criterios, dimensiones o comportamientos, necesarios de tomarse en cuenta, para realizar una tarea, controlar y evaluar detalladamente el desarrollo de un proyecto, evento, producto o actividad. Dichos componentes se organizan de manera coherente para permitir que se evalúe de manera efectiva, la presencia o ausencia de los elementos individuales enumerados o por porcentaje de cumplimiento u ocurrencia. (citado por Tongo, 2017 pag 80)

- ISO/IEC 27002 (2005, 2013)- Código de buenas prácticas para la Gestión de la Seguridad de la Información
- ENS - Esquema Nacional de Seguridad

Tabla N° 2
Técnicas e instrumentos

TÉCNICAS	INSTRUMENTOS	ELEMENTOS DE LA POBLACIÓN	DESCRIPCIÓN
Observación	Ficha de Observación	Activos de data center.	Con el uso de esta ficha se procederá al llenado de la observación indicando, los activos físicos del área Data Center del Hospital Regional de Ayacucho.
Encuestas	Cuestionario de encuestas	Personal del área	Este cuestionario estará dirigido al personal que labora en el área de informática, para recoger información acerca los activos del Área de Data Center, para así conocer y determinar los activos involucrados en la seguridad física.
Entrevistas	Cuestionario de entrevistas	Jefe del área Data Center	Cuestionario de entrevista estará dirigido al jefe con preguntas abiertas estuvo dirigido al encargado del dpto., para recoger información acerca de la seguridad física que existe en el área, para así conocer y determinar el nivel de conocimiento en temas de seguridad de información y en el uso de sus activos para preservar la seguridad se sus activos en totalidad.

Técnicas e instrumentos de la investigación

3.4.3 HERRAMIENTAS PARA LA ELABORACIÓN DEL PROCEDIMIENTO

La selección de la herramienta para la elaboración de los procedimientos de la auditoría de la investigación, de seguridad física del Data Center del Hospital regional de Ayacucho, es muy importante, por ello se ha tomado en cuenta las herramientas que son los más apropiados para problema de investigación, aquellas que se basan en las normas, regulaciones y busquen el mayor beneficio para la institución a Auditar. A continuación, se muestra los siguientes estándares, marcos de control de TI o normas. En la Tabla 3:

Tabla N° 3
Herramientas para la elaboración del procedimiento de auditoria

ESTANDARES	ELABORADO	USO
NTP-ISO/IEC 17799:2007	EDI (Comité Técnico de Normalización de codificación e Intercambio Electrónico de Datos). Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.	Es una guía práctica que desarrolla los estándares organizacionales de la seguridad y genera prácticas efectivas durante la gestión de la Seguridad de la Información. ofreciendo los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones.
COBIT 5.0	ISACA	COBIT fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI manteniendo un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo asumidos. COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos. COBIT 5 se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado, público o entidades sin fines de lucro

Herramienta para la elaboración de los procedimientos para realizar la auditoría en seguridad física del Data Center – Hospital Regional de Ayacucho.

CAPÍTULO IV

ANÁLISIS Y RESULTADOS DE LA INVESTIGACIÓN.

4.1 PROCEDIMIENTOS GENERALES DE AUDITORÍA EN SEGURIDAD FÍSICA DEL DATA CENTER DEL HOSPITAL REGIONAL DE AYACUCHO

Para realizar los procedimientos de Auditoría Física del Data Center del Hospital Regional de Ayacucho se desarrollarán mecanismos para establecer aspectos clave de Auditoría como son el alcance, el objetivo general y los objetivos específicos que serán considerados como criterios.

Ya determinados estos elementos de procedimientos de auditoría física, se indicará una serie de lineamientos que pueden ejercer de criterios para la auditoría del Data Center de Hospital Regional de Ayacucho de acuerdo al estándar y normas mencionados en la Tabla 3, los cual permite asegurar que se evaluarán los elementos necesarios de la Seguridad Física del Data Center.

Cabe aclarar que en cada etapa se presenta un análisis general el cómo se debe hacer la Auditoría y a continuación la aplicación de los procedimientos de auditoría en seguridad física para la "Hospital Regional de Ayacucho", con la finalidad de que se sustente las pruebas realizadas a los procedimientos de auditoría antes detallados en el presente trabajo de investigación.

4.2 DESARROLLO DE LA METODOLGIA

4.2.1 1ra Etapa: Planeación de la Auditoría

En esta 1ra etapa de la Auditoría física, se identifica el origen de la Auditoría; visita preliminar al Área que será evaluada; establecer los objetivos de la Auditoría; elaborar planes. programas y presupuestos; identificar y seleccionar métodos, procedimientos, instrumentos y herramientas; y asignar los recursos necesarios para la ejecución de la auditoría.

Siendo el objeto de estudio de Auditoría del Data Center, algunos factores que podrían estar involucrados en la evaluación son las siguientes:

- El mandato y el cometido de una de las entidades: Área de Control Interno, Gerencia General o área de auditoría interna.
- Políticas y procedimientos internos.
- Infraestructura.
- Leyes y regulación interna pertinentes al Hospital Regional de Ayacucho.
- Efectuar un seguimiento con las recomendaciones dadas en anteriores evaluaciones (Auditorías pasadas en caso exista)

En efecto estos factores podrían influir en la determinación del objetivo general de la auditoría, por tanto, la entrevista con estas áreas permitirá conocer cuáles son las incertidumbres que buscan cubrir con el resultado que se obtenga de la auditoría, los puntos en los que se encuentran involucradas las diferentes áreas para el funcionamiento y administración del Data Center y el motivo por el que creen se debe realizar una evaluación.

4.2.1.1 Determinación del Alcance de la Auditoría

La determinación del alcance de la auditoría es el primer paso cuando se ha decidido dar inicio a la misma, para la definición del alcance de la auditoría es necesario conocer la realidad del Data Center del Hospital Regional de Ayacucho. Ya que el alcance permitirá aclarar al auditado cuáles son los límites de la evaluación, de manera que los puntos a evaluarse sean los más críticos y que brinden una mejor visión de la realidad.

Es importante conocer cuáles son los elementos de auditoría física y adicional los elementos ambientales que pueden ser auditados, que ayudan al control de Auditoría Física en un Data Center por el cual a continuación en la tabla 4, se mencionan los aspectos que pueden ser auditados.

Alcance: La auditoría física y del entorno (medio ambiente) tendrá un alcance de todo el Data Center del Hospital Regional de Ayacucho, que está ubicada en parte posterior de dicha institución, teniendo como guía para el análisis los siguientes ítems:

a) Marco de control COBIT 5 (Dominios, Procesos y Objetivos relacionados a la seguridad Física)

b) La NTP-ISO/IEC 17799 (Dominio 9-Seguridad física y ambiental)

c) El periodo de visita a las instalaciones del Data Center comprende el 21 y 22 de octubre del 2019, previo acuerdo con el jefe del área de informática del Hospital.

4.2.1.2 Elementos Auditables y Elementos Ambientales de Seguridad Física

Los activos de seguridad física del Data Center que pueden ser auditados son aquellos que se relacionan con el cuidado Físico del Data Center, para su funcionamiento continuo, así como para proteger de incidentes naturales o personas malintencionadas.

a) Se tomarán en cuenta los elementos de seguridad física de la tabla 4 para el análisis de riesgo.

A continuación, se detallan en la tabla 4 los aspectos de seguridad física que pueden ser auditados:

Tabla N° 4
Elementos auditables de seguridad física del Data Center

ELEMENTOS AUDITABLES DE SEGURIDAD FÍSICA	
ELEMENTO	**DEFINICIÓN**
Grado de obsolencia	La obsolencia en los activos físicos puede ser factor muy perjudicial para la continuidad de servicios que ofrece el Data Center, ya que el desgaste de los equipos puede ocasionar problemas técnicos que afecten o indispongan el servicio. Es importante indicar dos términos relacionados con este punto de análisis: • **Obsolencia técnica:** Se refiere al tiempo excedido por el equipo de acuerdo al tiempo de vida determinado en la fabricación del mismo o de acuerdo a prácticas internacionales. • **Obsolencia por su uso:** El desgaste del equipo debido al tiempo que ha sido utilizado.
Ubicación	Acorde a las buenas prácticas de seguridad de información, la ubicación del Data Center, deben encontrarse alejados en un rango de al menos 2 Km. El objetivo de las buenas prácticas en la ubicación se da principalmente para evitar que, en un evento no previsto, como puede ser un incendio o terremoto, se vean comprometidas tanto las áreas funcionales, así como el Data Center, generando una pérdida total para la organización. Dentro de este punto, es importante considerar que el Data Center debe ubicarse en una zona donde se haya realizado previamente un análisis y que no sea riesgosa con respecto a desastres naturales, vibraciones, entre otros.

	El tamaño mínimo recomendado para un espacio que funcione como sala de equipos es de 13.5 **m^2**, en caso de no conocer el valor referencial es con un área de 0.07 **m^2** de espacio por cada 10 **m^2** de área de trabajo
Puertas de acceso	Las puertas deben ser de un material resistente a golpes y maltratos, se recomienda que sea estructurada con planchas de acero, refuerzos en su parte interna, cerraduras electromagnéticas, resistencia al calor de por lo menos 1000 ˚F por hora, de manera que para que ésta sea abierta deba verificarse que quien desea ingresar contar con los permisos necesarios para hacerlo, evitando el paso del personal mal intencionadas. De la misma forma, debe haber una sola forma de acceso al Data Center.
Cableado	Con respecto al cableado, debe contarse con una documentación correcta de los mismos, que facilite la realización de modificaciones o ampliaciones en el Data Center. Para lograr se pueden usar rack, gabinetes, canaletas, gabinetes y etiquetas.
Falso piso	La existencia de un falso piso busca proteger tanto a los equipos y como al cableado de incidentes que podría producir una inundación o fuga de agua en el edificio.
Documentación de procedimientos de asignación	Se debe guardar un registro físico y virtual de las asignaciones de permisos como de los dispositivos de seguridad asignados a los trabajadores, de manera que se pueda tener control sobre los mismos. Dentro de los dispositivos de seguridad para empleados o visitantes (proveedores, reguladores, auditores, clientes, entre otros.) están las tarjetas de identidad, llaves tipo tokens, contraseñas y demás
Dispositivos biométricos	Es necesario dotar al Data Center de la seguridad con los dispositivos biométricos, ya que de ella dependerá que personal no autorizado o capacitado ingrese a realizar maniobras en los equipos, lo que pudiese ocasionar fallas en el sistema y con ello brindando mayor seguridad. Estos dispositivos deben ser capaces, también, de registrar los intentos positivos y fallidos de ingreso.
Señalización	Los ingresos y salidas deben encontrarse señalizados ubicadas de forma adecuada, así como las áreas de alto voltaje o que cuentan con algún riesgo. Con esto no solo se busca cumplir con las regulaciones dadas por Defensa Civil, así como por el Ministerio de trabajo, sino también asegurar la salud y bienestar del personal de la organización.
Sistema de vigilancia	Se debe contar con un mecanismo de vigilancia permanente que permita controlar y conocer las acciones que se realizan alrededor y dentro del Data Center. Con ello se busca controlar las acciones que puedan ser perjudiciales para el mismo.

Sistema de red independiente	Es recomendable poseer un segmento de red totalmente independiente al del resto de la empresa para el uso exclusivo del Data Center. Con esto se busca evitar problemas que puedan producirse en la red debido a sobrecargas de trabajo, ingreso de virus que busquen apoderarse de información importante, entre otros, que provengan de alguna otra área de la empresa.
Desplazamiento libre	Los pasadizos y accesos del Data Center deben encontrarse libres para facilitar el desplazamiento del personal responsable, la salida del Data Center y para la instalación de nuevos equipos cuando sea necesario.
Programa de mantenimiento correctivo	Se debe contar con un programa que permita un control constante del estado y posibles inconvenientes que puedan producirse en los equipos del Data Center, tanto de los funcionales, así como de los equipos de respaldo.
ELEMENTOS AMBIENTALES QUE PUEDEN AFECTAR LA SEGURIDAD FÍSICA EN UN DATA CENTER	
ELEMENTO AMBIENTAL	**MEDIDAS DE SEGURIDAD**
Humedad • sensores de aniego	El mal funcionamiento del sistema de refrigeración puede generar la condensación de agua, esto puede causar el cortocircuito en el equipamiento, y como consecuencia el daño de os equipos. Por tato los sensores son equipos ubicados en el piso con el objetivo de poder detectar de forma temprana las inundaciones que puedan ocurrir en las instalaciones y que pueden afectar al Data Center.
Temperatura • Sistema de extinción de incendios	Se debe contar con sistemas de extinción que permitan resolver de manera rápida la ocurrencia de un incendio dentro del local del Data Center. Este sistema de extinción debe utilizar una tecnología acorde con la realidad del Data Center como son los materiales y el personal que trabaja en él.
• Detectores de humo	El estándar recomienda que se instale un sistema detector de humo para brindar un mejor nivel de protección al Centro de Datos. Los detectores de humo deben ser enlazados con el sistema de supresión de incendios, de manera que cuando éste detecte la presencia de partículas de humo se inicie el proceso de supresión de incendios inmediatamente.
• Detectores de humedad	Debido a un mal funcionamiento del sistema de refrigeración el ambiente puede generar la condensación de agua sobre los componentes, por tanto, estos dispositivos apoyan en la detección del nivel de humedad con el que cuenta el Data Center. El factor humedad puede ser muy perjudicial para el funcionamiento pues de tener valores muy elevados puede degradar el material de los equipos y de tener valores muy bajos producir energía estática.

• Refrigeración	Contar con equipos de aire acondicionado que permitan controlar la temperatura y humedad dentro de la sala de servidores, así como en las otras salas del Data Center.
• Pintura anti fuego	Un incendio en Data Center ocasionaría pérdidas de los bienes y datos, además conlleva a otras amenazas derivados como calor, humo, gases corrosivos entre otros por esta razón se debe contar con pintura anti fuego en las paredes permitirá disminuir y retardar los efectos que se generarían de producirse un incendio en el Data Center. Éste podrá controlar o disminuir el fuego, de acuerdo a sus características.
Suministro eléctrico	La energía eléctrica es indispensable para el funcionamiento de los equipos eléctricos y electrónicos en un ambiente Data Center, y la interrupción de este servicio ocasionaría la paralización del funcionamiento de los servicios del ambiente, por tal razón es necesario contar con un suministro de electricidad de respaldo, como son los grupos electrógenos, para asegurar la continuidad del negocio y el bienestar del personal que se encuentre dentro del Data Center frente a un corte eléctrico.
• Fluido eléctrico de respaldo	
• UPS	Se debe contar con equipos UPS (sistema de alimentación ininterrumpida) con la capacidad suficiente para permitir la autonomía necesaria para el encendido del grupo electrónico.
Polvo	En el ambiente de Data Center se pueden presentar la inadecuada calidad de aire que puede poner en riesgo al personal y fallas en los quipos por la obstrucción de filtros, ventiladores por la acumulación de polvo. En efecto estos dispositivos permitirán determinar cuándo los equipos están siendo invadidos por el polvo, de manera que se pueda tomar acciones y evitar que éste pueda deteriorar los equipos.
• **Sensores de polvo**	
Magnetismo	La correcta ubicación y distribución de los cables eléctricos y de red ayudaran a evitar la interferencia que podría producirse entre ellos, generando pérdida de datos, interferencia en la comunicación o errores en la transmisión.
• Adecuada ubicación de cables	

Elementos auditables de la Seguridad Física y elementos ambientales que pueden afectar la Seguridad Física en un Data Center.

4.2.1.3 Desarrollo del Objetivo General de la Auditoría Física

Definido el alcance de la auditoría física se procede a desarrollar el objetivo de la misma. El objetivo general regula de manera holística lo que se pretende evaluar, este será complementado por los objetivos específicos denominados por los estándares 27001, NTP 17799 como criterios de auditoría. La auditoría a la que va dirigido el presente informe de

investigación es eminentemente el de verificar la seguridad física del Data Center del Hospital Regional de Ayacucho.

Objetivo General: Realizar la evaluación de la infraestructura del Data Center del Hospital Regional de Ayacucho, para verificar la disposición de la Seguridad Física con la que cuenta sus instalaciones actualmente.

Conocimiento preliminar del Data Center del HRA:

Tabla N° 5
Datos generales de la entidad a Auditar

DATOS GENERALES		ENTIDAD
Nombre de la Institución	**:**	Hospital Regional de Ayacucho
Área responsable	**:**	Área de Informática
Área a auditar	**:**	Área de Data Center
Administrador del Data Center	**:**	Jefe del Área-Wilber Aguirre Landeo Personal del Área: Juan Manuel Chávez
Auditor	**:**	Bach. Vilca Dipaz Abel

Datos generales de la entidad a ser auditado

Materiales para la ejecución de la auditoría: Carpeta de trabajo, cámara digital.

¿Cuál es el soporte del Data Center al Hospital Regional de Ayacucho? ¿Su funcionamiento es 24 horas del día, los 7 días de la semana y los 365 días al año?

El Data Center aloja y da soporte a los sistemas de SIGA (Sistema Integrado de Gestión Administrativa), SIAF (Sistema Integrado de Administración Financiera), Galenhos, Lolcli, Bbcore Y Biomed. También servicios de telefonía IP e internet. El funcionamiento del Data Center es requerido de manera crítica los días laborales (lunes a viernes y en horarios de oficina). Para el mantenimiento no cumple el 24x7x365 porque a veces los domingos un lapso de media hora se apaga los sistemas que no se utilizan por ejemplo Galenhos.

¿En cuanto a la Seguridad Física, Existen políticas, procedimientos formales y normas de acceso en el Data Center?

No se cuenta con ninguna documentación de políticas ni de normas de seguridad para el Data Center. Pero si existe una política interna para el área de informática que se hizo en el año 2010.

¿se tiene la documentación sobre la construcción e instalaciones del Data Center?

Si, el Data Center fue implementado hace 9 años parte de un proyecto, en cuya documentación se tienen las especificaciones técnicas de los equipos a adquirir en ese entonces; la construcción del local no fue examinado, la parte posterior del Hospital fue el ambiente asignado, porque éste era el lugar cerca a las demás oficinas para la implementación del Data Center. La documentación está a cargo del área.

¿Las contratas que se realiza en los procesos de mantenimiento preventivo y correctivo en el Data Center? ¿estas cuentan con seguros de riesgo?

No, no se cuenta con ningún seguro de riesgo y el mantenimiento se hace tres veces al año previa acuerdo con área de informática.

4.2.2 2da ETAPA: EJECUCIÓN DE LA AUDITORÍA

En esta 2da etapa desarrollamos los procedimientos. Siguiendo la metodología mencionada en esta investigación. Se desarrolla los siguientes: realizamos acciones programadas para la Auditoría; aplicamos instrumentos y herramientas para la Auditoría e integrar el legajo de papeles de trabajo de la auditoría realizada.

4.2.2.1 Definición de los Criterios a seguir en la Auditoría

Partiendo de los objetivos y alcance previstos y considerando toda la información obtenida, se procederá a escoger los criterios que serán planteados según la norma NTP-ISO/IEC 17799 :2007, el marco de control COBIT 5.0, todos éstos enfocados en los aspectos de seguridad física del Data Center del HRA y así dar inicio a la elaboración del cuadro de criterios (Ver Anexo D).

4.2.2.2 Levantamiento y/o Recolección de Evidencias para la Auditoría

En este punto de la auditoría Física se busca los medios o caminos por las cuales se podrá realizar el levantamiento de evidencias. como propósito se tiene en cuenta los siguientes aspectos: De acuerdo a los criterios elegidos para dar inicio a la auditoría, según el Control de Objetivos para Tecnologías de Información y Relacionadas (COBIT 5.0) y la norma NTP-ISO/IEC 17799, será necesario evaluar los controles relacionados a ellos y proceder con el

levantamiento de evidencias. Una vez seleccionados los controles a evaluar se procede a la recolección y evaluación de evidencias, para lo cual será necesaria la clasificación de los controles:

Tabla N° 6
Clasificación de los controles

CONTROLES	
No existentes	**Existentes**
Son necesarios aplicarlos, pero al realizar la Auditoría podrían no ser identificados	Son identificados al momento de realizar la Auditoría y requieren ser evaluados para verificar si cumplen con su funcionamiento

Vamos hacer uso de las siguientes técnicas mencionados para evaluar los controles existentes.

- Observación
- Encuesta
- Entrevista
- Análisis documental
- Conciliación; contrastar la información con personas o documentos, como pueden ser:
    - ✓ Los reportes de auditorías pasadas en relación a seguridad Física (en este caso se va tomar en cuenta los inventarios realizados).
    - ✓ Revisión de documentos acerca de la seguridad física.

Al realizar la recopilación de información para la evidencia tomamos en cuenta:

- Depurar toda la información recopilada que no es de nuestro interés.
- Calificación de la persona que suministra la información o evidencia, que tenga un buen entendimiento del área técnica que está en revisión, de lo contrario la información recopilada puede ser no confiable.
- Objetividad de la evidencia: la evidencia se debe entender sin ningún tipo de explicación o interpretación.
- Toda la información obtenida debe ser manejada de forma confidencial y ética.

Para determinar la validez del instrumento se utilizó la técnica de juicio de expertos, donde se eligieron 2 especialistas, Ingenieros en Sistemas con títulos de Magíster, versados en el tema, quienes a través de un formato de validación como se ilustra en el Anexo C: Estructura de la Entrevista

Entrevista realizada al administrador del Data Center:

Nombre de la Organización	: Hospital Regional de Ayacucho
Área a entrevistar	: Data Center
Dirigido	: Jefe del área
Ciudad	: Ayacucho-Huamanga
Dirección	: Av. Independencia N° 355 del Distrito de Ayacucho

Tema de Investigación:
"AUDITORÍA PARA EVALUAR LA SEGURIDAD FÍSICA DEL DATA CENTER DEL HOSPITAL REGIONAL DE AYACUCHO, 2019"

Objetivo:
El cuestionario que se presenta a continuación está orientado a los trabajadores del Área de Estadística e Informática para determinar la importancia de hacer una Auditoria de Seguridad Física al Data Center del Hospital Regional de Ayacucho, el impacto de esta investigación tendrá dentro de Área, la identificación de amenazas-vulnerabilidades y la probabilidad que estos se materialicen.

1. **¿Existen políticas y procedimientos formales de Seguridad Física del Data Center del Hospital Regional de Ayacucho?**

No, no existe una política sobre seguridad física que contempla el control de accesos al Data Center, así como el comportamiento dentro de él, pero se tiene una política interna en el área de interna que se documentó en el año 2010. Para el ingreso y mantenimiento del Data Center es trato directo con el jefe del área.

2. **¿Cómo se sociabiliza con los usuarios estas políticas y procedimientos?**

Hay dos trabajadores que están permanente en el área. Que ya conocen las políticas del área en caso que se incorpore un trabajador, practicante o visita de personas externos, se les da a conocer estas políticas y procedimientos, pero no se cuenta con un documento en digital para difundirlo a todo el personal, ni tampoco se cuenta con una actualización de dichas políticas desde el año 2010.

3. **¿en cuanto a la documentación de las políticas y procedimientos, cuáles son los mecanismos de seguridad con la que se le da la salvaguarda?**

Desde el momento en que documentó, este permanece en el área de informática y otro de respaldo es un área que no se pueden indicar su ubicación por cuestiones de seguridad.

4. **¿Para La documentación de las políticas y procedimientos de seguridad del Hospital Regional de Ayacucho, cuáles son las condiciones de ambiente en las cuales están almacenadas?**

La documentación está almacenada en el área de informática a cargo el jefe del área. Por cuestiones de confidencialidad no se pueden indicar exactamente ni dar copias de estos documentos

5. **¿Existe un área específica para la seguridad física del Data Center?**

No, ya que todo lo referente a la seguridad en TI son actividades que debe cubrir mi puesto. Yo realizo los procedimientos de seguridad y las coordinaciones con terceros para el mantenimiento preventivo y correctivo.

6. **¿Cuáles son los procedimientos de acceso al Data Center Hospital Regional de Ayacucho?**

Ninguna persona puede tener acceso al área del Data Center sin previa autorización del jefe del área. En la actualidad dos personas tienen la llave de acceso jefe y un personal de confianza del. Para el acceso de terceras personas se solicita la identificación y la finalidad por la que se desea ingresar. Y fuera del horario de la oficina hay personal de seguridad merodea el área.

7. **¿Se realiza el monitoreo y revisión de las bitácoras, de ser así cada que tiempo se realiza?**

Nosotros solo almacenamos las bitácoras en carpetas, de ser necesario revisarlas solo se busca la carpeta requerida como: contrato para el mantenimiento, autorización para el ingreso de los materiales entre otros.

8. **¿Se evalúa el reporte de accesos al Data Center, de ser así este monitoreo con qué frecuencia se realiza?**

No, no se realiza un monitoreo de estos reportes, porque no se ha implementado aun un sensor de detección de entrada al área.

9. **¿Se cuenta con sensores de Control ambiental para él Data Center?**

No, no contamos con ningún sistema de sensores de controles ambientales. para los servidores contamos con dos equipos de aire acondicionado dos UPS y los reguladores de energía con pozo a tierra trifásica

10. ¿Se cuenta con políticas y procedimientos para elegir a los proveedores?

Sí, pero estos solo los maneja el área de abastecimiento, solo para el tema de mantenimiento y preventivo y correctivo se cuenta con dos proveedores. En caso de que se requiera algún equipo o servicio nosotros generamos las cotizaciones con los proveedores y realizamos una solicitud correspondiente para enviarla a abastecimiento ellos se encargan de realizar el contrato.

4.2.2.3 Identificar los Activos

Después de definir los criterios a continuación se identifican los activos físicos que se encuentran en el Data Center del Hospital Regional de Ayacucho, dichos activos serán ubicados en la tabla "activos físicos de un Data Center" Tabla B.1 (ver Anexo B)

4.2.2.4 Realizar la Tasación de los Activos

Después de ser identificados se procede a realizar la tasación de activos físicos, la calificación se hará en términos de la "disponibilidad", puesto que se evalúa la seguridad física del Data Center del Data Center del Hospital Regional de Ayacucho. El criterio de la calificación se da según la tabla E.3 (Anexo E) aplicando la pregunta ¿Cómo una pérdida o falla de un determinado activo afecta su disponibilidad? "Los valores asignados a la disponibilidad de cada uno de los activos se deducen del análisis de la importancia de dicho activo para la realización de las funciones o procesos indispensables para las actividades que realiza la entidad auditada. Este criterio se fundamenta en el análisis de impacto al negocio. Estos parámetros corresponden al criterio del auditor con la ayuda del análisis de impacto al negocio" (Llerena & Navarro, 2013). En la tasación de activos se utilizará la tabla E.2 (Anexo E).

4.2.2.5 Identificación de las Amenazas y Vulnerabilidades

El siguiente paso es la identificación de las Amenazas y Vulnerabilidades que se presenta en los activos físicos del Data Center, cabe indicar que las amenazas se seleccionan en base al objetivo de la Auditoría, es decir las que pueden afectar al normal funcionamiento del Data Center en relación directa con la Infraestructura Física y entorno del mismo (se toma en cuenta los elementos de Seguridad Física presentados en la Tabla 4.

4.2.2.6 Cálculo de las Amenazas y Vulnerabilidades

En este paso se procede a realizar la estimación de la Probabilidad de las Amenazas. Para determinar la probabilidad se debe analizar las vulnerabilidades que pueden ser explotadas por alguna de las amenazas listadas. Para determinar la "probabilidad de ocurrencia de una amenaza frente a una vulnerabilidad" (ver tabla D.4 del Anexo D) con la lista de vulnerabilidades indicadas vamos a determinar la probabilidad de ocurrencia mediante un cuestionario que permitirá conocer el tipo de controles que existen en el Data Center. esta estimación se va a determinar en base a la escala de Likert (Tabla 1).

4.2.2.7 Análisis y Evaluación de Riesgo

Después de calcular las amenazas y vulnerabilidades procedemos a valorar el riesgo; para ello haremos uso de la "Matriz de riesgo" (ver tabla E.5 del anexo E): Los activos identificados en la Tabla E.1, en la columna "Activos". valores obtenidos en la tasación de cada uno de los activos en base a la importancia que representa en términos de disponibilidad, se ubicarán en la matriz de riesgos en la columna "Impacto" (consideremos que el impacto va unido con la disponibilidad del activo). Para valorar el riesgo multiplicamos el impacto por la probabilidad. Una vez obtenido la valoración del riesgo, se identificará aquellos que tienen mayor riesgo en el Data Center, y procedemos a priorizarlos de mayor a menor. Por último, se presentará las conclusiones del análisis de riesgo y las acciones a tomar en cuenta.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Realizamos el análisis de riesgo siguiendo los pasos establecidos en marco teórico en el capítulo **2- sección 2.2.9:**

A. **Identificación de activos** encontrados en el Data del hospital Regional de Ayacucho (identificamos los activos por ficha de observación, cuestionario de encuesta y ficha de entrevista). para este cuadro se utiliza el anexo E Tabla E.1

Tabla N° 7
Activos físicos del Data Center del Hospital Regional de Ayacucho

ACTIVOS FISICOS QUE SE ENCUENTRAN EN UN DATA CENTER			
GRUPO	**EQUIPO PARA UNIDAD DE INFORMATICA**	**CANTIDAD**	**CARACTERISTICAS/DESCRIPCION**
Sala de servidores	servidores	7	Se cuenta con servidores de Sistema Gestión Hospitalaria, sistemas de gestión administrativa y de cortafuegos
	Líneas Telefónicas	2	Características comunes
	Central telefónica		No se cuenta con un central telefónico
	Dispositivos de almacenamiento (HDD externos)	5	Disco duro de 1 TB
	Racks	2	Soporte metálico que aloja los servidores y equipos de comunicación.
	Ups	4	Potencia de 1000 VA y 5000 VA.
	Regulador de energía	4	Es un dispositivo electrónico diseñado para mantener un nivel de tensión constante. Los servidores cuentan con uno cada uno
	Gabinete de pared		
	Aire acondicionado	2	Aire acondicionado con medidor de temperatura, humedad de ambiente,
	laptop		Intel Corei5 2.30 Ghz. 8.00 GB. Windows 8.1 32 Bits
	Pc Escritorio	2	Disco Duro 500 GB. Intel Corei3 3.40 Ghz. Memoria 4.00 GB. 64 bits
Equipos de red	Switches	4	2 Switches Core y 2 de distribución. de 24 salidas y 16 salidas. Negociación a 10/1 00/1 000 Mbps
	Routers	4	Routers de telefónica. 2,4 GHz + 5 GHz dual concurrente 1,93 Gbps 802.11ac
	Patch panels	2	Cat. 5 y 6 Mod. 24 puertos color negro
	Cables de red		Cable de Fibra óptica, cable UTP de categoría 5 y otras de categoría 6.

B. Tasación de Activos: Para la tasación se realizó la pregunta ¿De qué manera una pérdida, falla técnica de un activo Físico puede afectar la disponibilidad y servicios que brinda el Data Center?; para esta evaluación se utiliza la tabla E.2 (del anexo E), para el valor del activo se hace referencia a la tabla E.3 del anexo E

Dado que el objetivo principal de la Auditoria, es evaluar la seguridad Física del Data Center, se considera únicamente el atributo "Disponibilidad" en la tasación de activos, con el propósito de asignar un grado de valor según la importancia que representa que se encuentre disponible

dicho activo para los objetivos de la entidad, el cual se asignará acorde a la tabla E.4 del anexo E:

Tabla N° 8
Tasación de activos físicos del Data Center

N°	ACTIVOS FÍSICOS DEL DATA CENTER	VALOR
1	Servidores	5
2	Líneas Telefónicas	2
3	Dispositivos de Almacenamiento (HDD externos)	5
4	Racks	2
5	Ups	5
6	Regulador de Energía	5
7	Aire Acondicionado	5
8	Laptop	3
9	Switches	4
10	Routers	4
11	Patch Panels	3
12	Cables De Red	3
13	pc escritorio	1

Tasación de activos físicos del Data Center del Hospital Regional de Ayacucho.

Estos valores asignados a la Disponibilidad de cada uno de los activos físicos del Data Center se deducen del análisis de la importancia de dicho activo para la realización de las funciones o procesos indispensables para las actividades que realiza el Hospital Regional de Ayacucho.

C. Identificación de las Amenazas y Vulnerabilidad

En este paso se identifican las Amenazas y Vulnerabilidades, a continuación se presenta la tabla de amenazas de tipo Físico presentes en el Data Center del Hospital Regional de Ayacucho, cabe indicar que las amenazas se seleccionan en base al objetivo de la de Auditoría realizada al área mencionado, es decir las que pueden afectar al normal funcionamiento del Data Center en relación directa con la Infraestructura Física del mismo.

Tabla N° 9
Amenazas al entorno del Data Center - HRA

N°	AMENAZAS
01	Temperatura inadecuada
02	Presencia de Humedad
03	Falta de refrigeración y fallas de circulación de aire
04	Acceso de personal no autorizado
05	Incendios

06	Tormentas/rayos
07	Perdida de energía
08	Filtraciones de agua (lluvias, tuberías averiadas), inundaciones entre otros
09	Sismos
10	Huelga y vandalismo
11	Polvo y suciedad
12	Error humano y/o Pérdida del personal
13	Contaminación de gases y/o partículas
14	Documentación insuficiente del cableado

Amenazas para el Data Center del Hospital Regional de Ayacucho.

Tabla N° 10
Principales vulnerabilidades del Data Center-HRA

N°	VULNERABILIDADES
01	Infraestructura ubicada en la parte posterior del establecimiento de salud HRA
02	Espacio y distribución de equipos no diseñados correctamente
03	Paralización de aire acondicionado por perdida de energía
04	Existe material peligroso (cartones apilados) dentro del Data Center
05	Falta de mantenimiento periódico de los UPS
06	Falta de Extintores del incendio en los pasadizos.
07	Falta de cámaras de seguridad
08	Paredes sin protección contra la humedad
09	Paredes revestidas sin elementos ignífugos
10	Aire acondicionado con antecedentes de fallas
11	Puerta del Data center sensible a actos violentos
12	Paredes sin condiciones de estabilidad térmica
13	Paredes, pisos y techos no sellados ni pintados con un material de reducción y aparición de polvo
14	No existe un dispositivo de detección de polvo
15	Elementos almacenados en la entrada (cajas de cartón, armarios de madera), sensibles a desprender fibras o polvo al ser manipulados
16	Administrador del Data Center con exceso de trabajo
17	Personal con insuficiente formación en administración técnica del Data center, sensible a cometer negligencia o equivocaciones.
18	No existe detectores de elementos químicos como gases
19	No existe sistema de circuito cerrado de televisión.

20	No existe equipo detector de humo.
21	No existe equipo sensor de humedad.
22	Falta de mantenimiento y limpieza frecuente en el local y equipos del Data Center
23	No existe bocas de incendio equipadas próximas a la entrada del Data Center
24	Piso, paredes, equipos y techos con acumulación de polvo
25	Existencia de grabaciones de CD y DVD
26	Condiciones e instalación del cableado eléctrico y de red.
27	Control personal de limpieza en locales con servidores.
28	Switches, Pantalla de configuración y Routers inestables
29	Etiquetado inadecuado de medios de energía y de datos
30	Descarga eléctrica en los equipos, Desprendimiento de instalaciones en azoteas, techos débiles que caen y cortan cables.
31	No existe control biométrico para el acceso la data center

Principales vulnerabilidades encontradas en el Data Center del Hospital Regional de Ayacucho

D. Cálculo de las Amenazas y Vulnerabilidad

Tabla N° 11
Cálculo de las Amenazas y Vulnerabilidades del Data Center-HRA

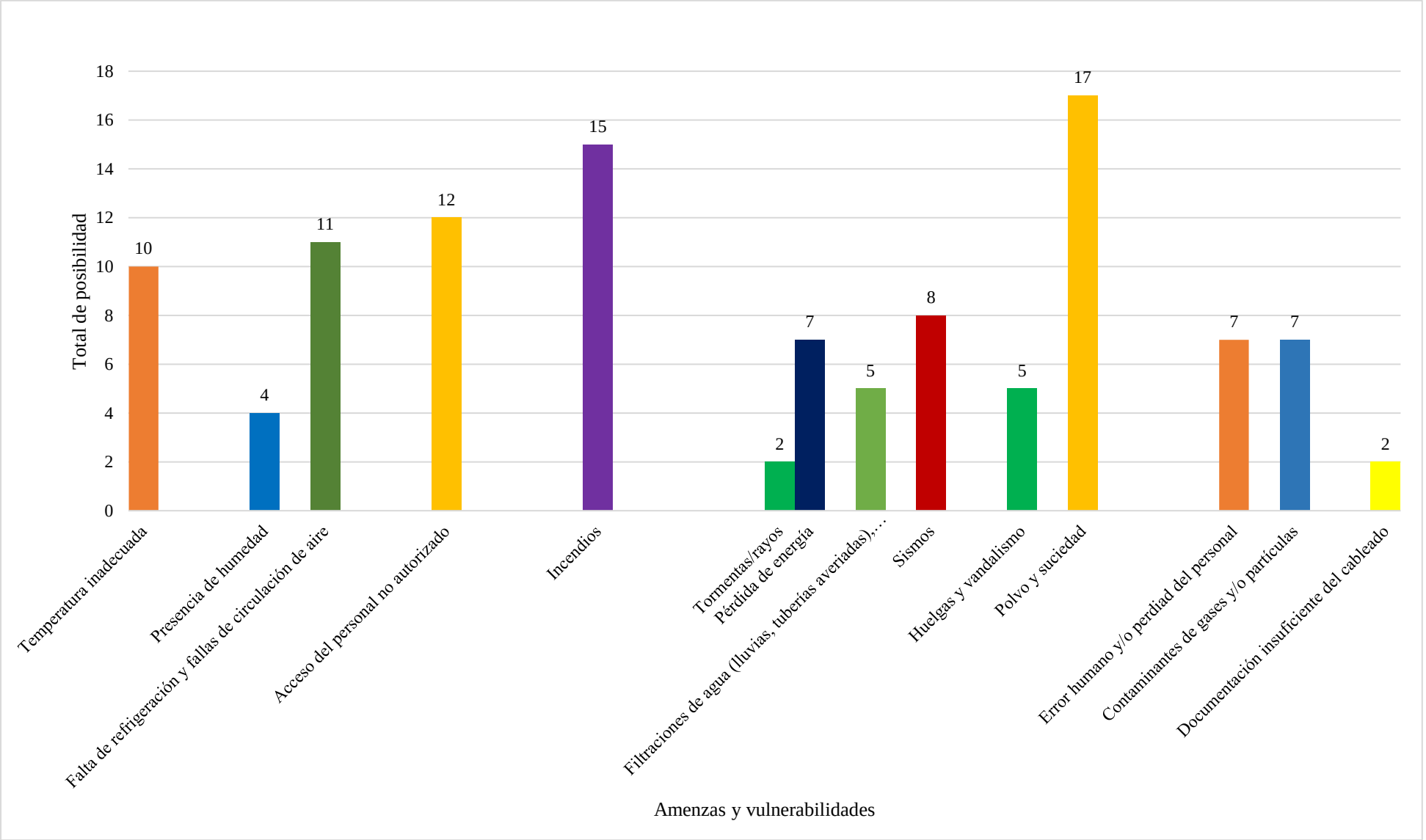
N°	AMENAZAS	VULNERABILIDADES	Probabilidad de Ocurrencia	Total
01	Temperatura inadecuada	Aire acondicionado con antecedentes de fallas	3	10
		Paralización de aire acondicionado por perdida de energía	4	
		Equipos de aire acondicionado de confort sensible a fallas.	2	
		Paredes sin condiciones de estabilidad térmica	1	
02	Presencia de humedad	No existe equipo sensor de humedad.	2	4
		Paredes sin protección contra la humedad	2	
03	Falta de refrigeración y fallas de circulación de aire	Espacio y distribución de equipos no diseñados correctamente	2	11
		Aire acondicionado con antecedentes de fallas	3	
		Piso, paredes, equipos y techos con acumulación de polvo	2	
		Falta de mantenimiento y limpieza frecuente en el local y equipos del Data center	4	
04	Acceso del personal no autorizado	No existe sistema de circuito cerrado de televisión	2	12
		Falta de cámaras de seguridad	3	
		Existencia de grabaciones de CD y DVD	2	
		No existe control biométrico para el acceso la data center	3	
		Control personal de limpieza en locales con servidores	2	
05	Incendios	Existe material peligroso (cartones apilados) dentro del Data Center	3	15
		Paredes revestidas sin elementos ignífugos	2	
		Falta de Extintores del incendio en los pasadizos.	3	
		Elementos almacenados en la entrada (cajas de cartón, armarios de madera), sensibles a desprender fibras o polvo al ser manipulados	2	
		No existe equipo detector de humo	2	

		No existen bocas de incendio equipados próximas a la entrada del Data center	3	
06	Tormentas/rayos	Descarga electrica en los equipos, Desprendimiento de instalaciones en azoteas, techos débiles que caen y cortan cables.	2	2
07	Pérdida de energía	Condiciones e instalación del cableado eléctrico	3	7
		Falta de mantenimiento periódico de los UPS	4	
08	Filtraciones de agua (lluvias, tuberías averiadas), inundación entre otros	Infraestructura ubicada en parte posterior del establecimiento	2	5
		No existe equipo sensor de humedad.	3	
09	Sismos	Aire acondicionado con antecedentes de fallas	2	8
		Falta de mantenimiento y limpieza frecuente en el local y equipos del Data Center	3	
		Switches, Pantalla de configuración y Routers inestables	3	
10	Huelgas y vandalismo	Puerta del Data center sensible a actos violentos	3	5
		Infraestructura ubicada en local posterior del hospital regional de Ayacucho	2	
11	Polvo y suciedad	Paredes, pisos y techos no sellados ni pintados con un material de reducción y aparición de polvo	2	17
		No existe un dispositivo de detección de polvo	3	
		Elementos almacenados en la entrada (cajas de cartón, armarios de madera), sensibles a desprender fibras o polvo al ser manipulados	4	
		Piso, paredes, equipos y techos con acumulación de polvo	4	
		Falta de mantenimiento y limpieza frecuente en el local y equipos del Data Center.	4	
12	Error humano y/o pérdida del personal	Administrador del Data Center con exceso de trabajo	4	7
		Personal de administración del Data Center con insuficiente formación técnica, sensible a cometer negligencia o equivocaciones.	3	
13		Falta de mantenimiento periódico de los UPS	2	7

	Contaminantes de gases y/o partículas	Elementos almacenados en la entrada (cajas de cartón, armarios de madera), sensibles a desprender fibras o polvo al ser manipulados	4	
		No existe detectores de elementos químicos como gases	1	
14	Documentación insuficiente del cableado	Etiquetado inadecuado de medios de energía y de datos	2	2

Cálculo de la probabilidad de que una amenaza ejecute una vulnerabilidad del Data Center del Hospital Regional de Ayacucho.

Gráfico 1: cálculo de posibilidad de ocurrencia Amenazas y Vulnerabilidades del Data Center-HRA



E. Análisis De Riesgo y su Evaluación.

Tabla N° 12
Matriz de riesgos del Data Center

MATRIZ DE RIESGOS		AMENAZAS													
		Temperatura inadecuada	Presencia de humedad	Falta de refrigeración y falta de circulación de aire	Acceso del personal no autorizado	Incendios	Tormentas/ rayos	Pérdida de energía	Filtraciones de agua (lluvias, tuberías averiadas), inundación entre otros	Sismos	Huelgas y vandalismo	Polvo y suciedad	Error humano y/o pérdida del personal	Contaminantes de gases y/o partículas	Documentación insuficiente del cableado
Probabilidad de amenaza		**10**	**4**	**11**	**12**	**15**	**2**	**7**	**5**	**8**	**5**	**17**	**7**	**7**	**2**
Activo	**Impacto**	**VALORACION DE LOS RIESGOS**													
Servidores	5	50	20	55	60	75	10	35	25	40	25	85	35	35	10
Líneas Telefónicas	2	20	8	22	24	30	4	14	10	16	10	34	14	14	4
Dispositivos de Almacenamiento (HDD externos)	5	50	20	55	60	75	10	35	25	40	25	85	35	35	10
Racks	2	20	8	22	24	30	4	14	10	16	10	34	14	14	4
Ups	5	50	20	55	60	75	10	35	25	40	25	85	35	35	10

Regulador de Energía	5	50	20	55	60	75	10	35	25	40	25	85	35	35	10
Aire Acondicionado	5	50	20	55	60	75	10	35	25	40	25	85	35	35	10
Laptop	3	30	12	33	36	45	6	21	15	24	15	51	21	21	6
Switches	4	40	16	44	48	60	8	28	20	32	20	68	28	28	8
Routers	4	40	16	44	48	60	8	28	20	32	20	68	28	28	8
Patch Panels	3	30	12	33	36	45	6	21	15	24	15	51	21	21	6
Cables De Red	3	30	12	33	36	45	6	21	15	24	15	51	21	21	6
pc escritorio	1	10	4	11	12	15	2	7	5	8	5	17	7	7	2

Matriz de riesgos del Data Center del Hospital Regional de Ayacucho.

E.1 PRIORIZACIÓN DE LOS RIESGOS:

Se estableció en función de los resultados que se obtuvo en la tabla 12 "*Matriz de riesgos del Data Center*", las amenazas pueden ser priorizadas en orden descendente con base en su factor de exposición al riesgo.

Tabla N° 13
Priorización de Riesgos

Amenazas	Polvo y suciedad	Incendios	Acceso del personal no autorizado	Falta de refrigeración y falta de circulación de aire	Temperatura inadecuada	Sismos	Pérdida de energía	Error humano y/o pérdida del personal	Contaminantes de gases y/o partículas	Filtraciones de agua (lluvias, tuberías averiadas), inundación entre otros	Huelgas y vandalismo	Presencia de humedad	Tormentas/rayos	Documentación insuficiente del cableado
Activos	**Priorización**													
	1	2	3	4	5	6	7	7	7	8	8	9	10	10
Servidores	85	75	60	55	50	40	35	35	35	25	25	20	10	10
Dispositivos de Almacenamiento	85	75	60	55	50	40	35	35	35	25	25	20	10	10
Ups	85	75	60	55	50	40	35	35	35	25	25	20	10	10
Regulador de Energía	85	75	60	55	50	40	35	35	35	25	25	20	10	10
Aire Acondicionado	85	75	60	55	50	40	35	35	35	25	25	20	10	10
Switches	68	60	48	44	40	32	28	28	28	20	20	16	8	8
Routers	68	60	48	44	40	32	28	28	28	20	20	16	8	8
Laptop	51	45	36	33	30	24	21	21	21	15	15	12	6	6
Patch Panels	51	45	36	33	30	24	21	21	21	15	15	12	6	6
Cables De Red	51	45	36	33	30	24	21	21	21	15	15	12	6	6
Líneas Telefónicas	34	30	24	22	20	16	14	14	14	10	10	8	4	4
Racks	34	30	24	22	20	16	14	14	14	10	10	8	4	4
pc escritorio	17	15	12	11	10	8	7	7	7	5	5	4	2	2

Priorización de los riesgos del Data Center del Hospital Regional de Ayacucho. Fuente: Autor

4.2.3 3ra ETAPA: DICTAMEN DE LA AUDITORÍA

4.2.3.1 Documentación de Hallazgo

Los hallazgos es el resultado de la comparación y evaluación de las evidencias contra los criterios que hayan sido determinados de acuerdo a los objetivos de Auditoría, pudiendo así establecer si fue o no conforme con los criterios establecidos.

Las evidencias a buscar para la obtención de los hallazgos deben ser, cumplir los objetivos, las cuales corresponden ser evaluadas siguiendo los criterios de auditoría definidos anteriormente.

Figura N° 12 Ilustración del hallazgo.

Para este caso, la documentación de hallazgos consistirá en describir las evidencias para el usuario como para el auditor, la realidad encontrada al evaluar la existencia o no, con los criterios y el cumplimiento de los objetivos de estos criterios dentro del Data Center, y de poseer evidencias que sean útiles para justificar los resultados a los que llegue el auditor y al mismo tiempo para servir de guía de mejora al área evaluado.

En efecto los hallazgos encontrados durante la auditoría podrán ser clasificados, en los siguientes grupos:

1. **Si hay hallazgo:** Este escenario se da cuando el cumplimiento del criterio relacionado es del 100%, es decir:

   a. Existe un control para el criterio del aspecto auditado en el Data Center,

   b. Adicionalmente la disponibilidad del control es la adecuada.

   c. Está dimensionado la infraestructura de forma correcta, contando con el número suficiente y necesario de componentes tecnológicos de apoyo.

2. **No conformidad:** Cuando el criterio evaluado no ha sido cumplido en su totalidad.

3. **Insuficiente:** Cuando existe un control relacionado a un criterio específico, pero sin embargo

   a. El control carece de eficiencia o disponibilidad a un nivel menor que podría afectar la continuidad del negocio del administrador del Data Center.

   b. No está dimensionado la infraestructura de forma correcta, en el número suficiente y necesario.

Después de clasificar los hallazgos en los tres grupos, también es necesario identificar la evidencia para los grupos "No conformidad" e "Insuficiente" de acuerdo a la criticidad, para demostrar la importancia del levantamiento de los hallazgos correspondientes.

El documento de hallazgos será la guía que permita al cliente identificar las desviaciones de los objetivos de control que inicialmente se estableció, por otro lado, planificar las actividades de carácter correctivo que se consideren convenientes para subsanarlas.

4.2.3.2 Levantamiento de Evidencias y Documentación de Hallazgo

Criterios considerados en la auditoría de la seguridad Física del Data Center

- Dominio 9 de la NTP-ISO/IEC 17799:2013 (refiérase 9 .1.1, 9 .1.2, 9 .1.4, 9.1.5, 9.1.6, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.6, 9.2.7)
- El marco de control COBIT 5.0 (refiérase EDM01, APO01.02, APO0 1.07, APO07.O 1, APO 1 0.03, APO 12.05, BAI03.07, BAI03.08, BA106.02, DSS01.04, DSS02.04, DSS02.05, DSS04.01, DSS04.07, DSS05.05, DSS05.07)

A continuación, desarrollamos los criterios basados en NTP-ISO/IEC 17799

Tabla N° 14
Dominio y Criterios NTP-ISO/IEC 17799

DOMINIO	**9. SEGURIDAD FÍSICA Y DEL ENTORNO (AMBIENTAL)**
CRITERIOS	**9.1 Áreas Seguras**
	Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.
	9.2 Seguridad de los equipos
	Evitar pérdidas, daños o comprometer los activos, así como la interrupción de las actividades de la organización.

Dominio y Criterios de NTP-ISO/IEC 17799 para levantamiento de evidencias del Data Center del Hospital Regional de Ayacucho. Fuente: (ISO/IEC - INDECOPI, 2014)

Calificación porcentual (CP) = Calificación Total (CT)*100/Ponderación Total (PT)

Tabla N° 14. 1
Evidencias y Hallazgos del control-perímetro de Seguridad Física

CONTROL	**9.1.1 Perímetro de seguridad Física**
	Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados para proteger el área

a) El perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física. Los muros externos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados;

Evidencias	Cumplimiento	Hallazgo	Recomendación
La infraestructura es de material solido (Concreto)	Si cumple		

b) Se debería instalar un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería restringir sólo al personal autorizado;

Evidencias	Cumplimiento	Hallazgo	Recomendación
No existe ninguna área de recepción manual para el Data Center.	No cumple	Data Center sin ninguna área de recepción manual para el acceso	Tener un área de recepción manual manejado por el área de informática, para registrar ya sea la fecha, hora del ingreso, entre otros datos de las personas ajenos que ingresan al Data Center

c) Las barreras físicas se deberían extender, si es necesario, desde el suelo real al techo real para evitar entradas no autorizadas o contaminación del entorno;

Evidencias	Cumplimiento	Hallazgo	Recomendación
No existen barreras físicas, porque el ambiente del Data Center fue adecuado en una infraestructura ya existente.	No cumple	Data center sin barreras físicas en su Edificación.	Se recomienda si en un futuro se decide realizar el traslado de todo el Data Center a una infraestructura nueva, se debe tener en cuenta la construcción de barreras.

d) Todas las puertas para incendios del perímetro de seguridad deberían tener alarma, ser monitoreadas y probadas;

Evidencias	Cumplimiento	Hallazgo	Recomendación

No existe puertas con alarmas de incendio	No cumple	Data center sin alarma de incendios	En caso de hacer una nueva infraestructura tener en cuenta la instalación de estos equipos
e) Se debe instalar sistemas adecuados de detección de intrusos. de acuerdo a estándares regionales, nacionales o internacionales			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No existe ningún dispositivo de detección de intrusos. Solo es el personal de seguridad	No cumple	Data center sin sistema de detección de intrusos	Se debe instalar el sistema de detección de intrusos
TOTAL =CP*PT	**20%**	**Cumplimiento:** Optimo (CP= (100*100%) /5), No cumple (0%) y parcial (10%)	

Control-Perímetro de seguridad Física, para Levantamiento de evidencias y hallazgo del Data Center del HRA

Tabla N° 14. 2

Evidencias y Hallazgos del control- Controles físicos de entradas

CONTROL	**9.1.2 Controles físicos de entradas**
	Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado.

a) Las visitas a las áreas seguras se deberían supervisar, a menos que el acceso haya sido aprobado previamente, y se debe registrar la fecha y momento de entrada y salida. Los visitantes sólo tendrán acceso para propósitos específicos;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Las visitas a las áreas se realizan en compañía del personal encargado del área; pero no existe un registro de fecha/hora de ingreso y salida de las visitas.	Parcial (16.67%)	Se entra al área con un acuerdo verbal	Debe existir un mecanismo de control. Contar con registro de visitas, previa solicitud al área especifico
b) Se debería controlar y restringir sólo al personal autorizado el acceso a la información sensible y a los recursos de su tratamiento; usar controles de autenticación, mantener un rastro auditable de todos los accesos;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**

El ingreso que se hizo al Data Center mediante un candado. Cuya llave está a cargo del administrador	Parcial (16.67%)	No cuenta con control de ingreso auditable	Se recomienda control de acceso biométrico

c) Se debería exigir a todo el personal que lleve puesta alguna forma de identificación visible y se le pedirá que solicite a los extraños no acompañados y a cualquiera que no lleve dicha identificación visible, que se identifique;

Evidencias	Cumplimiento	Hallazgo	Recomendación
No hay exigencia de identificación visible. Pero si se identifican verbalmente al jefe del área	Parcial (16.67%)	Personal no identificado visiblemente no genera confusión con el personal de la institución	Se recomienda al personal, identificación visible como: fotocheck de la misma manera a las personas ajenas de la institución
TOTAL =CP*PT	**50%**	**Cumplimiento:** Optimo (CP= (100*100%) /3), No existe (0%) y parcial (16.67%)	

Control- Controles físicos de entradas, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 3

Evidencias y Hallazgos del control- Protección contra amenazas externas y ambientales

CONTROL	**9.1.4 Protección contra amenazas externas y ambientales**
	Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana, del Data Center del Hospital Regional de Ayacucho.

a) Los materiales peligrosos y combustibles se deberían almacenar en algún lugar distante de las áreas seguras;

Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Se observó del material inflamable (papeles, maderas, cajas de cartón) a la entrada del Data Center.	Parcial (16.67%)	Los materiales fácilmente inflamables no están distantes del Data Center.	Se recomienda en un corto plazo buscar otro espacio para los materiales inflamables que se encuentran a la entrada del Data Center.

b) El equipo y los medios de respaldo deberían estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal;

Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No existe otro ambiente para los medios de respaldo (está en estudio). El respaldo se guarda en la misma área.	Parcial (16.67%)	El encargado indica la importancia de albergar los medios de respaldo en nuevo local.	Tener un medio de respaldo fuera del área principal

c) Equipo apropiado contra incendio debe ser provisto y ubicado adecuadamente

Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No existe un equipo adecuado contra incendios.	Parcial (16.67%)	Hay un extintor en el Data Center	Contar con equipos contra incendios como: detector de humo, extintores ubicados adecuadamente

TOTAL =CP*PT	**50%**	**Cumplimiento:** Optimo (CP= (100*100%) /3), No existe (0%) y parcial (16.67%)

Control- Protección contra amenazas externas y ambientales, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 4

Evidencias y Hallazgos del control- El trabajo en el Data Center

CONTROL	**9.1.5 El trabajo en el Data Center**		
	Se debería diseñar y aplicar protección física y pautas para trabajar en el área de Data Center		
a) Debería evitar el trabajo no supervisado en áreas seguras tanto por motivos de salud como para evitar oportunidades de actividades maliciosas;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Todos los trabajos son supervisados por el personal del área	Si cumple		
b) No se debería permitir la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial.			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No se permiten fotografiar, filmar. Pero en ocasiones especiales permite con la autorización del administrador	Si cumple		
TOTAL =CP*PT	**100%**	**Cumplimiento:** Optimo (CP= (100*100%) /2), No existe (0%) y parcial (25%)	

Control- El trabajo en el Data Center, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 5

Evidencias y Hallazgos del control- Acceso público, áreas de carga y descarga

CONTROL	**9.1.6 Acceso público, áreas de carga y descarga**		
	Se deberían controlar las áreas de carga y descarga, y si es posible, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.		
a) deberían restringir los accesos al área de carga y descarga desde el exterior únicamente al personal autorizado e identificado;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
La compra de equipos está a cargo de unidad de abastecimiento del Hospital Regional de Ayacucho	Si cumple		
a) El área de carga y descarga se debería diseñar para que los suministros puedan descargarse sin tener acceso a otras zonas del edificio;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**

El área esta al lado de otras áreas del establecimiento de salud	Parcial	El área de abastecimiento está lejos del Data Center, pero si cerca a otras áreas	Diseñar un área específica para la recepción de suministros
TOTAL =CP*PT	**75%**	Cumplimiento: Optimo (CP= (100*100%) /2), No existe (0%) y parcial (25%)	

Control- Acceso público, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 6

Evidencias y Hallazgos del control- Instalación y protección de equipos

CONTROL	**9.2.1 Instalación y protección de equipos**
	El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.

a) Los controles deben ser adoptados para minimizar los riesgos de posibles amenazas como robo, incendio, explosivos, humo, agua (o fallo de suministro), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas y vandalismo;

Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No registra documentos de controles de los equipos	No cumple		Desarrollar mecanismos de controles físicos para los equipos

b) La organización debería incluir en su política cuestiones sobre fumar, beber y comer cerca de los equipos de tratamiento de información;

Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No existe políticas de comportamiento establecidas para el Data Center.	No cumple		Incluir en las políticas de seguridad de la Institución, los modos de comportamientos sobre fumar, beber y comer entre otros, dentro o próximos del Data Center

c) Se deberían vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información;

Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Existe un dispositivo para controlar la temperatura del medio ambiente mas no la humedad	Parcial	El encargado verifica la temperatura del Data Center cada cierto tiempo	Poner un horario en el día para la revisión de la temperatura en los ambientes del Data Center.
TOTAL =CP*PT	**16.67%**	Cumplimiento: Optimo (CP= (100*100%) /3), No existe (0%) y parcial (16.67%)	

Control- Instalación y protección de equipos, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 7
Evidencias y Hallazgos del control- Suministro eléctrico

	9.2.2 Suministro eléctrico		
CONTROL	Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo.		
a) Todas las instalaciones de apoyo, como la electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado debe ser adecuado;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Hay un tablero de distribución de energía Eléctrica en la puerta. El administrador mencionó que no existe suministro de agua ni desagüe en el Data center; el aire acondicionado está ubicado en parte central superior del área. El aire acondicionado tiene algunas fallas a la fecha	Parcial (10%)	Las fallas del aire acondicionado podrían ocasionar mayores conflictos a futuro. La ubicación del Aire acondicionado no ayuda a que haya una correcta circulación del aire.	establecer en un corto plazo los periodos de mantenimiento del aire acondicionado, aunque presente o no falla y en un en largo plazo se recomienda renovar el equipo de aire acondicionado.
b) Se recomienda instalar un Sistema de Alimentación Ininterrumpida (U.P.S.) para apoyar un cierre ordenado o el funcionamiento continuo de los equipos que soporten operaciones críticas del área;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Si existe un UPS para contrarrestar los cortes de energía inesperado. También existe un generador de energía.	Si cumple (20%)		
c) Además, se deberían instalar interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No existen interruptores de emergencia. Pero si las luces de emergencia.	Parcial (10%)	No hay instalaciones de interruptores de emergencia.	Instalar interruptores de emergencia que estén ubicados en zonas de rápido y fácil acceso.
d) El suministro de agua debe ser estable y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados);			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No existe el suministro de agua.	No cumple (0%)		hacer un análisis de las instalaciones de suministro de agua en el Data Center, para que en un futuro se adquieren equipos que requieran de agua y contemplar en dicho análisis que sus instalaciones sean estables.

e) Los equipos de telecomunicación deben ser conectados al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Solo existe una línea proveedor de datos	Parcial (10)	Hay proveedor de línea de telefónica	Contar con dos líneas de proveedor de datos
TOTAL =CP*PT	**50%**	Cumplimiento: Optimo (CP= (100*100%) /5), No existe (0%) y parcial (10%)	

Control- Suministro eléctrico, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 8

Evidencias y Hallazgos del control- Seguridad del cableado

CONTROL	**9.2.3 Seguridad del cableado**		
	Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.		
a) Las líneas de energía y telecomunicaciones en el Data Center, se deberían enterrar, cuando sea posible, o adoptarse medidas alternativas de protección;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Algunos cables de energía y telecomunicaciones se encuentran al aire libre, pero otros están con protección de corrugado.	Parcial (10%)	No todas las líneas de energía y de telecomunicaciones están con protección adecuada	Organizar el cableado estructurado haciendo uso del piso falso y/o canaletas.
b) Se deberían separar los cables de energía de los de comunicaciones para evitar interferencias;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Las instalaciones de los cables de energía y de datos están separada	Si cumple (20%)		
c) Cables claramente identificados y marcas de equipo deben ser utilizadas con el fin de minimizar errores de manejo como el de parchar cables de una red incorrecta;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Los cables no se encuentran etiquetadas. el administrador indica que lo reconocen por el color	Parcial (10%)	La falta de identificación de los cables. (sin etiqueta)	Se recomienda etiquetar los cables para minimizar errores en caso que ocurriese una falla inesperada
d) Una lista documentada de parches debe utilizarse con el fin de reducir la posibilidad de errores;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**

No existe un documento de los mantenimientos que se hizo en cuanto a los parches d ellos cables	No cumple (0%)	Tener un registro documentado de los parches realizados en el cableado de datos o de energía

e) Se deberían considerar medidas adicionales como: uso de rutas o de medios de transmisión alternativos; uso de cableado de fibra óptica; uso de un escudo electromagnético para proteger los cables, entre otros.

Evidencias	Cumplimiento	Hallazgo	Recomendación
El cableado estructurado no se encuentra muy ordenada, el material del cable si es resistente (cable de datos de categoría 6).	Parcial (10%)	El cableado desordenado no permitirá apreciar claramente que cables transitan de forma paralela, y éstas pueden producir interferencia de datos.	Tener una administración adecuada del cableado manteniendo el tipo de organización de cableado horizontal y vertical.
TOTAL =CP*PT	**50%**	Cumplimiento: Optimo (CP= (100*100%) /5), No existe (0%) y parcial (10%)	

Control- Seguridad del cableado, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 9

Evidencias y Hallazgos del control- Mantenimiento de equipos

CONTROL	**9.2.4 Mantenimiento de equipos**
	Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.

a) Los equipos se deberían mantener de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del suministrador;

Evidencias	Cumplimiento	Hallazgo	Recomendación
El administrados indica que los mantenimientos se realizan 3 veces al año	Parcial (12.5%)	No se realizan los mantenimientos de acuerdo a las especificaciones técnicas del suministrador.	establecer periodos fijos de mantenimiento de equipos; de acuerdo a las especificaciones técnicas del suministrador y para ello mantener un inventario actualizado de todos los activos del Data Center.

b) Sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y servicio de los equipos;

Evidencias	Cumplimiento	Hallazgo	Recomendación
El administrador menciona que algunas reparaciones lo realizan el mismo con el personal del área y otros contratan a terceros previa autorización	Cumple (25%)		

c) Se deberían registrar documentalmente todos las fallos, reales o sospechados, así como todo el mantenimiento preventivo y correctivo;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Se realiza documentación del mantenimiento realizado por los terceros no se documenta el mantenimiento correctivo y preventivo	Parcial (12.5%)	No registran documentos de acciones correctivos y preventivos; tampoco se registran los fallos reales y sospechosos	Se debería elaborar un plan de mantenimiento preventivo y correctivo y también se debe registrar un todas las fallas reales y sospechosos.
d) Se debería implementar controles apropiados cuando el equipo es programado para mantenimiento, tomando en cuenta si este mantenimiento es realizado por personal interno o externo del área; donde sea necesario, debe despejarse la información sensible del equipo;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
El mantenimiento de equipos del Data Center se realiza tres veces al año indica el administrador.	Parcial (12.5%)	El mantenimiento lo realiza el personal del área y también terceros mediante una contrata.	Elaborar controles de mantenimiento para los equipos como: • Intervalos de visitas técnicas: • Personal de mantenimiento. • Verificación del estado y funcionamiento de los equipos. • Periodos de Limpieza de los equipos.
TOTAL =CP*PT	**62.5%**	Cumplimiento: Optimo (CP= (100*100%) /4), No existe (0%) y parcial (12.5%)	

Control- Mantenimiento de equipos, para Levantamiento de evidencias y hallazgo del Data Center del HRA

Tabla N° 14. 10

Evidencias y Hallazgos del control- Seguridad en el rehúso o eliminación de equipos

CONTROL	**9.2.6 Seguridad en el rehúso o eliminación de equipos**
	Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.

a) Los dispositivos de almacenamiento con información sensible se deberían destruir físicamente o la información debe ser destruida, borrada o sobrescrita usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Los dispositivos de almacenamiento dañados se almacenan en el área para después ser entregados al área de patrimonio. No existe procedimientos que	Parcial (25%)	Los equipos como CD. Disco duro entre otros dispositivos, están a cargo del área de informática,	Incluir en las políticas de seguridad del Data del Center procedimientos que contemplen técnicas seguras de resguardo o de destrucción física de los dispositivos de almacenamiento.

contemplen las acciones técnicas de destrucción física de los dispositivos de almacenamiento (hasta la fecha no se ha realizado ninguna depuración de ningunos dispositivos de almacenamiento.		algunos ya entregado al área de patrimonios	
b) Los dispositivos dañados que contienen data sensible pueden requerir una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
No existe ningún documento de evaluación de riesgos de dispositivos dañados.	No cumple (0%)		cuando se dé el caso, realizar una evaluación de riesgos de aquellos dispositivos dañados que tengan da sensible; antes de ser descartados
TOTAL =CP*PT	**25%**	Cumplimiento: Optimo (CP= (100*100%) /2), No existe (0%) y parcial (25%)	

Control- Seguridad en el rehúso o eliminación de equipos, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

Tabla N° 14. 11

Evidencias y Hallazgos del control- Retiro de la propiedad

CONTROL	**9.2.7 Retiro de la propiedad**		
	El equipo, información o software no debe ser sacado fuera del local sin autorización		
a) El equipo, información o software no debe ser sacado fuera del local sin autorización;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
La extracción y retiro de cualquier equipo del Data Center es realizada previa autorización del jede de área de informática	Si cumple (25%)		
b) Los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos deben ser claramente identificados;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
El encargado del área y el personal de seguridad tienen conocimiento del personal	Si cumple (25%)		

que laboran en caso de personas ajenas entran previa autorización del administrador			
c) Los tiempos límite para el retiro de equipos deben ser fijados y el retorno del equipo verificado para asegurar la conformidad;			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
Los tiempos límites para el retorno de los equipos son fijados, y el responsable es directamente el administrador.	Si cumple (25%)		
d) El equipo debe ser registrado, si es necesario y apropiado, cuando este sea removido fuera del local, así como cuando sea devuelto.			
Evidencias	**Cumplimiento**	**Hallazgo**	**Recomendación**
El registro d ellos equipos es realizado por el encargado del área y otros por el área de patrimonio del establecimiento	Si cumple (25%)		
TOTAL =CP*PT	**100%**	Cumplimiento: Optimo (CP= (100*100%) /4), No existe (0%) y parcial (12.5%)	

Control- Retiro de la propiedad, para Levantamiento de evidencias y hallazgo del Data Center del HRA.

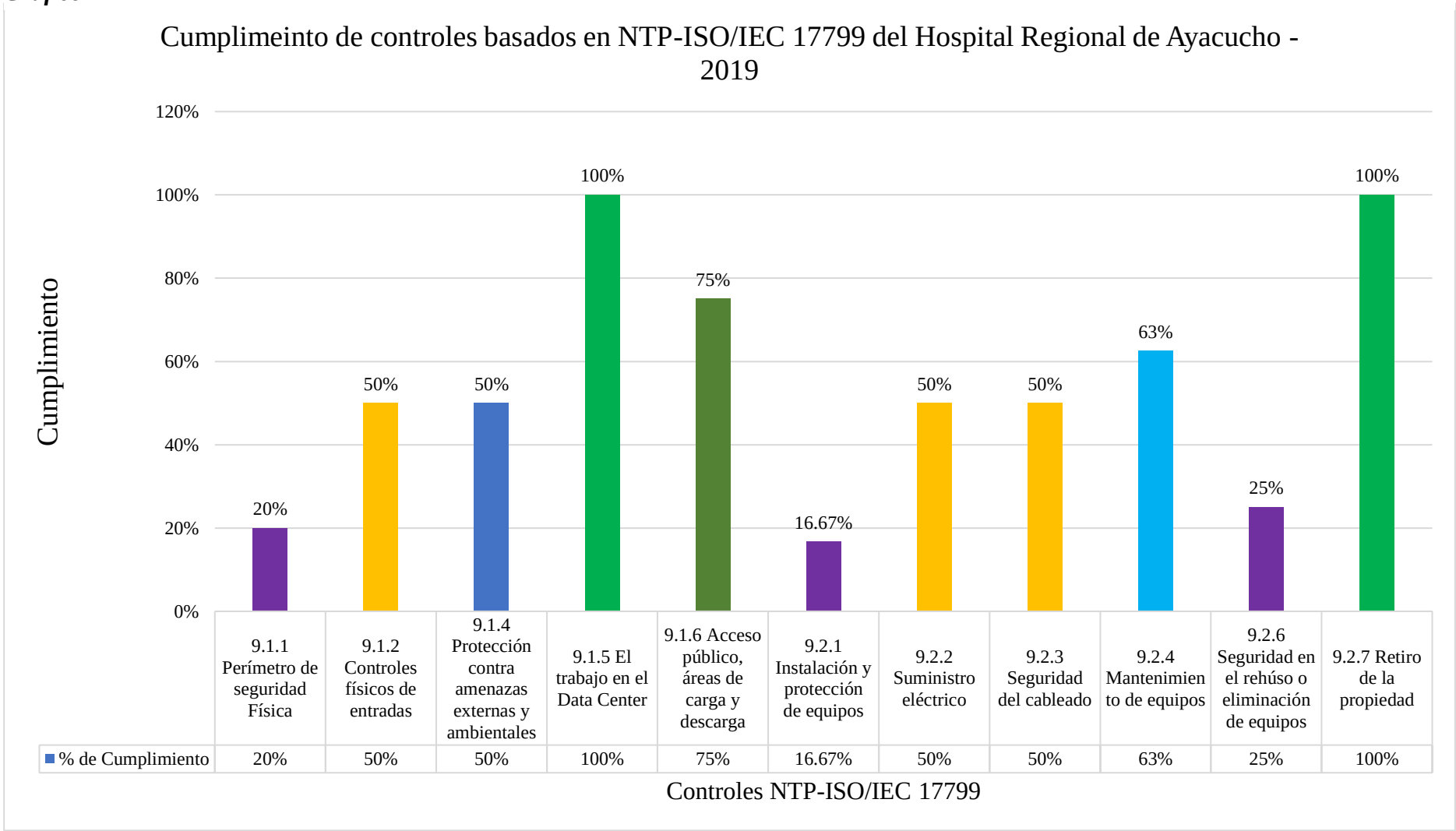
Tabla N° 15

Listado de Dominio y Criterios NTP-ISO/IEC 17799

DOMINIO	9. SEGURIDAD FÍSICA Y DEL ENTORNO (AMBIENTAL)	Cumplimiento (%)
	9.1.1 Perímetro de seguridad Física	
	9.1.2 Controles físicos de entradas	
	9.1.4 Protección contra amenazas externas y ambientales	
	9.1.5 El trabajo en el Data Center	
	9.1.6 Acceso público, áreas de carga y descarga	
Controles	9.2.1 Instalación y protección de equipos	
	9.2.2 Suministro eléctrico	
	9.2.3 Seguridad del cableado	
	9.2.4 Mantenimiento de equipos	
	9.2.6 Seguridad en el rehúso o eliminación de equipos	
	9.2.7 Retiro de la propiedad	

Lista de controles del NTP-ISO/IEC 17799 y su porcentaje de cumplimiento de los activos del Data Center – Hospital Regional de Ayacucho -2019

Gráfico 2


Cumplimeinto de controles basados en NTP-ISO/IEC 17799 del Hospital Regional de Ayacucho - 2019
Cumplimiento
120%
100%
80%
60%
40%
20%
0%
20%
50%
50%
100%
75%
16.67%
50%
50%
63%
25%
100%
9.1.1 Perímetro de seguridad Física
9.1.2 Controles físicos de entradas
9.1.4 Protección contra amenazas externas y ambientales
9.1.5 El trabajo en el Data Center
9.1.6 Acceso público, áreas de carga y descarga
9.2.1 Instalación y protección de equipos
9.2.2 Suministro eléctrico
9.2.3 Seguridad del cableado
9.2.4 Mantenimiento de equipos
9.2.6 Seguridad en el rehúso o eliminación de equipos
9.2.7 Retiro de la propiedad
% de Cumplimiento
20%
50%
50%
100%
75%
16.67%
50%
50%
63%
25%
100%
Controles NTP-ISO/IEC 17799

A continuación, desarrollo los criterios basados en COBIT 5

Tabla N° 16

Dominio de COBIT 5- Evaluar, Orientar y Supervisar (Gobierno)-EDM

Dominio	**Evaluar, Orientar y Supervisar (Gobierno)-EDM**		
	Asegura que los objetivos del Data Center sean logrados, evaluando las necesidades de los interesados		
Procesos	**EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno**		
	Verificar la existencia de un gobierno de seguridad física y ambiental en el Data Center de la institución		
	EDM05 Asegurar la transparencia hacia las partes interesadas		
	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de las TI de la empresa son transparentes		
Objetivos	**EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.**		
	Verificar la existencia de contratos que detallen los niveles de seguridad que el Data Center ofrecerá a los clientes.		
Descripción		**Cumplimiento**	**Recomendación**
El Data Center del Hospital Regional de Ayacucho no cuenta con políticas de seguridad física. Por su propia cuenta se capacitaron en temas comunes.		**No cumple** No existe políticas de seguridad que contribuyan con el gobierno de TI	Es de suma importancia programar las capacitaciones en seguridad física para el personal que administra el data center. La formación es esencial, porque los empleados que son capaces de reaccionar a los eventos no planificados pueden ayudar a evitar el tiempo de caída; por ello se recomienda entrenamiento y certificación formal.
TOTAL =CP*PT		**10%**	Cumplimiento: Optimo (CP= (100*100%) /1), No existe (0%) y parcial (50%)

Dominio de COBIT 5- Evaluar, Orientar y Supervisar (Gobierno)-EDM -procesos y objetivos de control para levantamiento de evidencias y hallazgos, del Data Center del Hospital Regional de Ayacucho

Tabla N° 17

Dominio de COBIT 5- Alinear, Planificar y Organizar (Gestión)-APO

Dominio	**Alinear, Planificar y Organizar (Gestión)-APO**		
	Este dominio proporciona la dirección para la entrega de soluciones y la entrega de servicios		
Proceso	**APO01 Gestionar el Marco de Gestión de TI**		
	Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.		
Objetivos	**APO01.02 Establecer roles y responsabilidades.**		
	Verificar el establecimiento de roles y responsabilidades en seguridad física del Data Center del HRA.		
Descripción		**Cumplimiento**	**Recomendación**

El establecimiento de roles y responsabilidades en seguridad física del Data Center es asignado de manera verbal para el jefe del área en caso de ausencia asume otro personal del área.	No cumple (0%) La asignación de los roles y responsabilidades no son formales.	Asignar un personal exclusivo para la administración del Data Center.

Proceso	**APO01.07 Gestionar la mejora continua de los procesos.**
	Verificar la ejecución de capacitaciones al personal encargado sobre las consideraciones de seguridad física del Data Center, cómo afectan a las operaciones del Hospital Regional de Ayacucho y las acciones a tomar en situaciones de riesgo.

Descripción	**Cumplimiento**	**Recomendación**
El personal no recibió una capacitación pertinente del tema de seguridad física del Data Center	No cumple (0%) El personal al no recibir una capacitación, no podrá responder eficientemente al cargo para lo cual fue contratado	Programar capacitaciones en seguridad Física para todo el personal que administra el Data Center

Proceso	**APO07 Gestionar los Recursos Humanos**
	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.
Objetivo	**APO07.01 Mantener la dotación de personal suficiente y adecuada.**
	Verificar la adecuada proporción entre recursos humanos y proveedores con respecto a los servicios que se ofrecen.

Descripción	**Cumplimiento**	**Recomendación**
El único responsable de administrar el Data Center, el jefe del área además éste cuenta con otras funciones El administrador manifiesta que la infraestructura del Data Center está creciendo.	Cumple parcialmente (10%) Se ocasiona conflictos en las labores de personal en caso de Presentarse necesidades urgentes dentro del Data Center.	Efectuar una cláusula que contemple las responsabilidades y roles correspondientes en el contrato del personal y/o coordinar con los responsables de recursos humanos o manejarlo a nivel interno.

Proceso	**APO10 Gestionar los Proveedores**
	Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos de equipos y servicios para el Data Center
Objetivo	**APO10.03 Gestionar contratos y relaciones con proveedores.**
	Verificar que los contratos con terceros o proveedores por lo menos deben incluir acuerdos de seguridad, acuerdos de confidencialidad**.**

Descripción	**Cumplimiento**	**Recomendación**
Los acuerdos con proveedores son por medio de contrato. Además de contar con certificación	Si cumple (20%)	

Proceso	**APO12 Gestionar el Riesgo**
	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa

Objetivo	APO12.05 Definir un portafolio de acciones para la gestión de riesgos del Data Center.	
Descripción	**Cumplimiento**	**Recomendación**
No hay conjunto de acciones para gestión de riesgos	No cumple (0%) No existe ninguna acción para gestión de riesgos del Data Center	Programar y llevar a cabo una evaluación anual de riesgos y amenazas que examine tanto las amenazas internas, como las externas del Data Center del Hospital Regional de Ayacucho
TOTAL =CP*PT	**30%**	Cumplimiento: Optimo (CP= (100*100%) /5), No existe (0%) y parcial (10%)

Dominio de COBIT 5- Alinear, Planificar y Organizar (Gestión)-APO-procesos y objetivos de control para levantamiento de evidencias y hallazgos, del Data Center del Hospital Regional de Ayacucho

Tabla N° 18

Dominio de COBIT 5- Construir, Adquirir e Implementar (Gestión)-BAI

Dominio	**Construir, Adquirir e Implementar (Gestión)-BAI**	
	La gerencia con este dominio pretende cubrir, que los nuevos proyectos generen soluciones que satisfagan las necesidades del Data Center	
Proceso	**BAI03. Gestionar la Identificación y Construcción de Soluciones.**	
	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes.	
Objetivos	**BAI03.07 Preparar pruebas de la solución**	
	Verificar la existencia de un plan de pruebas de soluciones en seguridad física y ambiental del Data Center.	
Descripción	**Cumplimiento**	**Recomendación**
No existe un plan de pruebas de soluciones	No cumple. (0%) La no existencia de prueba de soluciones. Genera un riesgo en la protección y mantenimiento de la infraestructura del Data Center.	Crear y/o definir un plan de pruebas. Para tener la capacidad y recuperación ante desastres
	BAI03.08 Ejecutar pruebas de la solución	
	Verificar si se han ejecutado las pruebas de soluciones en seguridad física de forma continua, identificando, registrando y dando prioridad a los errores y los problemas detectados durante las pruebas.	
Descripción	**Cumplimiento**	**Recomendación**
De acuerdo al detalle anterior no se puede dar este control	No existe (0%)	Tener un plan de pruebas de soluciones en Seguridad Física
Proceso	**BAI06 Gestionar los Cambios**	
	Gestiona todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura**.**	

Objetivo	**BAI06.02 Gestionar cambios de emergencia.**
	Verificar la existencia de mecanismos de emergencia que controlen el mantenimiento de los equipos del Data Center

Descripción	**Cumplimiento**	**Recomendación**
No existe mecanismos de emergencia que controlen el mantenimiento de los equipos	No cumple (0%) No hay mecanismos que controlen el mantenimiento de los equipos	Elaboración de procedimientos de emergencia parar responder a los diferentes incidentes que puedan amenazar los equipos del Data Center. Y que sean probados regularmente.
TOTAL =CP*PT		Cumplimiento: Optimo (CP= (100*100%) /5), No existe (0%) y parcial (10%)

Dominio de COBIT 5- Construir, Adquirir e Implementar (Gestión)-BAI -procesos y objetivos de control para levantamiento de evidencias y hallazgos, del Data Center del Hospital Regional de Ayacucho

Tabla N° 19

Dominio de COBIT 5- Entregar, dar Servicio y Soporte (Gestión) - DSS

Dominio	**Entregar, dar Servicio y Soporte (Gestión) - DSS**
	Es lograr que los servicios de TI se entreguen de acuerdo con las prioridades del Data Center, la optimización de costos, asegurar que la fuerza de trabajo utilice los sistemas de modo productivo y seguro, implantar de forma correcta la confidencialidad, la integridad y la disponibilidad.
Proceso	**DSS01 Gestionar Operaciones**
	Entregar los resultados del servicio operativo de TI, según lo planificado
Objetivo	**DSS01.04 Gestionar el entorno.**
	Verificar el cumplimiento de requisitos de gestión ambiental.

Descripción	**Cumplimiento**	**Recomendación**
No existe equipos que monitoreen los factores ambientales y accesos físicos del Data Center.	No cumple. (0%) Al no tener control no asegura que loes equipos estén protegidos	Implementar cámaras de seguridad que puedan grabar eventos fuera y dentro del data center.
Proceso	**DSS02 Gestionar las peticiones y los incidentes del servicio**	
	Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	
Objetivos	**DSS02.04 Investigar, diagnosticar y localizar incidentes.**	
Descripción	**Cumplimiento**	**Recomendación**
No existen procedimientos de gestión de incidentes y problemas.	No cumple (0%) El no tener un control de sus incidentes que se pueden convertir en Problemas serios.	Se recomienda contar con procedimientos de gestión de incidentes y problemas
Objetivos	**DSS02.05 Resolver y recuperarse de incidentes.**	
Descripción	**Cumplimiento**	**Recomendación**
No existe un plan de recuperación ante desastres. Solo se tiene los	Parcial (6.25%). Sin mecanismo de contrarreste los desastres que puedan ocurrir	Elaborar plan de recuperación ante desastres para asegurar, siempre en caso de un siniestro, la reconstrucción de la infraestructura del Data Center; Este

backup que realizan cada cierto tiempo		plan debe ser documentado y probado con periodicidad.
Proceso	**DSS04 Gestionar la Continuidad**	
	Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.	
Objetivos	**DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.**	
Descripción	**Cumplimiento**	**Recomendación**
No existe plan de continuidad actualmente	No cumple (0%).	Desarrollar un plan de continuidad basado en prevenir, reducir, recuperar y transferir. Este plan puede contener al plan de contingencia, también debe ser documentado y probado con periodicidad
	DSS04.07 Gestionar acuerdos de respaldo	
Descripción	**Cumplimiento**	**Recomendación**
Actualmente no se cuenta con un lugar estable de respaldo de datos	No cumple (0%). El área expresa su preocupación para adquirir un logar de almacenamiento de datos fuera de las instalaciones	Identificar un lugar de la institución que podrían ser adoptadas para el respaldo de los datos del Data Center
Proceso	**DSS05 Gestionar Servicios de Seguridad**	
	Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	
Objetivos	**DSS05.05 Gestionar el acceso físico a los activos de TI.**	
	Verificar la existencia de mecanismos de autorización y restricción de acceso a los locales del Data Center	
Descripción	**Cumplimiento**	**Recomendación**
El data center no está señalizada	No cumple (0%).	El área de Data Center debe tener una señalización correspondiente para su identificación. del personal del Establecimiento y no sea obvia para los visitantes
Objetivos	**DSS05.06 Gestionar documentos sensibles y dispositivos de salida.**	
	Verificar la existencia de garantías que aseguren y protejan la seguridad física y ambiental del Data Center.	
Descripción	**Cumplimiento**	**Recomendación**
Todo los Dispositivos adquiridos tiene una descripción de niveles de garantía y ambiental	Parcial (6.25%)	El administrador debe verificar con un experto los niveles de protección de la seguridad física y ambiental del Data Center
Objetivos	**DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.**	

	Verificar la existencia de herramientas de detección de intrusos para controlar el acceso no autorizado al Data Center.

Descripción	**Cumplimiento**	**Recomendación**
No existe ningún dispositivo para la detección de intrusos.	No cumple (0%). Al no contar con estos dispositivos se corre el riego de ser manipulado los equipos y datos del Data Center	Contar con los equipos de detención contra intrusos y alarmas.
TOTAL =CP*PT	**12.5%**	Cumplimiento: Optimo (CP= (100*100%) /8), No existe (0%) y

Dominio de COBIT 5-Entregar, dar Servicio y Soporte (Gestión) - DSS -procesos y objetivos de control para levantamiento de evidencias y hallazgos, del Data Center del Hospital Regional de Ayacucho

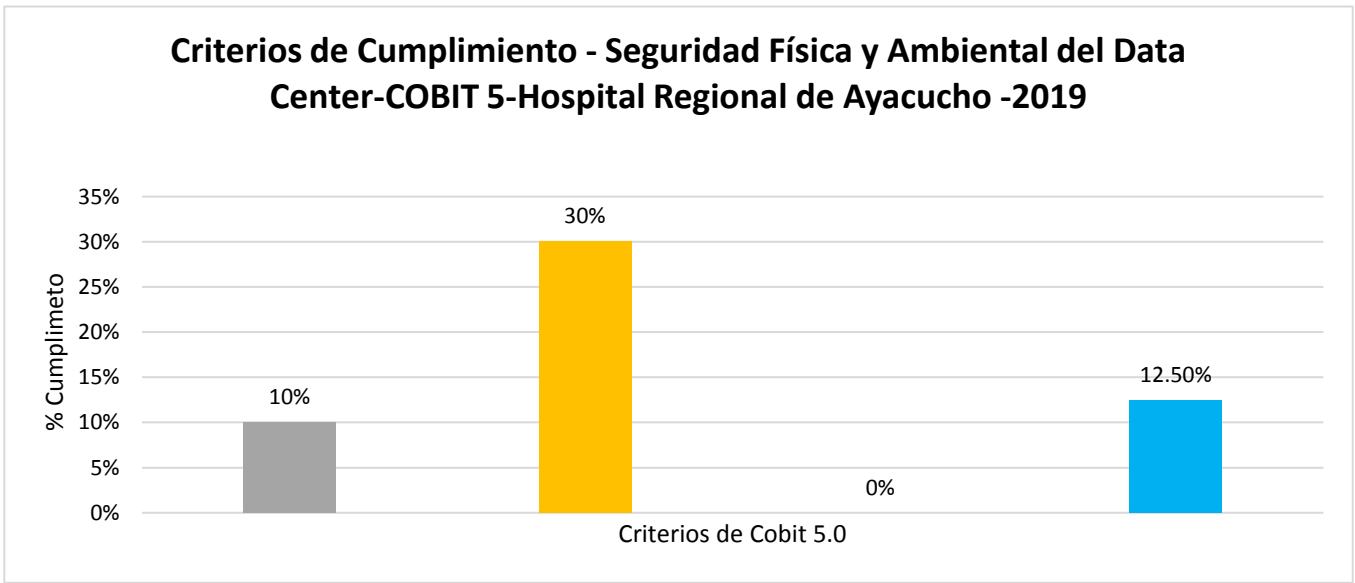
Tabla N° 20

Cumplimiento de los Controles de Seguridad Física y ambiental.

COBIT 5	Dominios-procesos-objetivos	% cumplimiento
Dominio	Evaluar, Orientar y Supervisar (Gobierno)-EDM-EDM01; EDM05.02	**10%**
	Alinear, Planificar y Organizar (Gestión)-APO-APO01.02; APO01.07; APO07.01; APO10.03; APO12.05	**30%**
	Construir, Adquirir e Implementar (Gestión)-BAI; BAI03.07; BAI03.08; BAI06.02	**0%**
	Entregar, dar Servicio y Soporte (Gestión) - DSS; DSS01.04; DSS02.04; DSS02.05; DSS04.01; DSS04.07; DSS05.05; DSS05.06; DSS05.07	**12.50%**

Cumplimiento de los criterios de los Dominios de COBIT 5, Seguridad Física y Ambiental del Data Center del Hospital Regional de Ayacucho

Gráfico 3



4.2.3.3 Documentación de las Conclusiones y Recomendaciones

En esta etapa final de la auditoría, después de haber definido los objetivos de la auditoría y haber evaluado la realidad física y medio ambiental del Data Center de acuerdo a un conjunto de criterios fijados a partir de la aplicación de normas y estándares internacionales de seguridad de información (NTP-ISO/IEC 17799, COBIT 5.0), se da por concluido el proceso de evaluación también conocido como auditoría de campo. Y por consiguiente se hace la documentación de conclusiones y recomendaciones.

Las conclusiones representan el resultado de la evaluación realizada; sin embargo, éstas deben poseer el detalle adecuado de los controles pendientes de mejora en el Data Center.

Los hallazgos son la base del detalle de estas conclusiones. De acuerdo al grupo al que hayan pertenecido según la clasificación mencionada anteriormente se deberá manifestar cada conclusión de acuerdo al siguiente contexto:

- **El criterio sí se cumple:** En este caso, no existe diferencia entre el criterio y la evidencia encontrada, por lo cual se deberá indicar comparativamente:

→ Norma o estándar internacional (apartado en particular de alguna de ellas) involucrado en el criterio.

→ El criterio mismo.

→ Y el control que está cumpliendo, la realidad del Data Center, tanto con la norma como con el criterio de la auditoría.

- **El criterio no se cumple:** En el caso de los criterios que no son cumplidos, se deberá clasificar el impacto de cada uno los hallazgos distinguiendo aquellos que corresponden a la seguridad física y aquellos que lo hacen para seguridad medio ambiental.
- **El criterio es insuficiente:** Al igual que en el caso de criterios no cumplidos, se deberá clasificar cada hallazgo de acuerdo al impacto que tenga en la seguridad, indicando los motivos por los cuáles no ha sido cumplido.

Este detalle nos servirá como guía, permitiéndonos conocer los puntos que se han auditado y el nivel de cumplimiento que el Data Center evaluado tiene con respecto a los criterios seleccionados.

Así como se debe documentar las conclusiones, otra labor de la auditoría es manifestar las recomendaciones adecuadas que le permitan solucionar los problemas encontrados.

A CONCLUSIONES DEL ANÀLISIS NTP-ISO/IEC 17799 Y COBIT 5.0

A.1. Del Análisis de riesgo realizado en la sección 4.2.2.7 se concluye:

Después de definir los niveles de riesgos respecto a las vulnerabilidades de cada activo y las amenazas que puedan afectar su disponibilidad, integridad y la disponibilidad; se Recomiendo medidas a tomarse en cuenta, desde los niveles de riesgos más altos hasta los más bajos (Ver tabla 13)

Tabla N° 21
Medidas de control para minimizar los riesgos en el Data Center.

Priorización	Amenazas	Controles Generales	Controles Específicos
1	Polvo y suciedad	Reducir y evitar la presencia del polvo	Realizar mantenimiento de limpiezas en: piso, paredes y techos.
			parte exterior del rack y todos los equipos del Data Center
			Interior de los Racks y todas las superficies de los equipos, canalizaciones, conductos, etc.
2	Incendios	Tener equipos y verificar las medidas de seguridad contra incendios	Instalar interruptores para detener una descarga accidental.
			Verificar que existe suficiente cantidad de extintores en el Data Center y el entorno
			Instalar sistemas de extinción de incendios y verificar regularmente el funcionamiento
3	Acceso del personal no autorizado	Aumentar las medidas de Seguridad en control de Acceso	Instalar cámaras de seguridad que puedan grabar dentro y fuera del Data Center
			Verificar que el personal de seguridad esté disponible en las entradas del Establecimiento
			desarrollar y probar procedimientos de emergencia para la seguridad del Data Center
			Instalar Sistema de seguridad Biométrico en la entrada del Data Center
4			verificar el buen funcionamiento del Aire acondicionado

	Falta de refrigeración y falta de circulación de aire	verificar la calidad del aire y los sistemas de aire Acondicionado	los sistemas de climatización sean revisados periódicamente al menos uno a mes
5	Temperatura inadecuada	Monitorear la temperatura	Adquirir equipo sensor de temperatura
			monitorear la temperatura del día
6	Sismos	Proteger los equipos que están en riesgo y los más sensibles	desarrollar y probar procedimientos de emergencia para el caso de sismos
7	Pérdida de energía	Controlar las interrupciones controlar la interrupción del suministro eléctrico.	Verificar las instalaciones de los cables de Poder
			verificar los UPS
			Verificar que este suministrado el equipo generador eléctrico
	Error humano y/o perdida del personal	Capacitación y apoya en el trabajo del administrador para minimizar los errores por negligencia	Solicitar capacitaciones del personal la seguridad Física del Data Center
			Diseñar políticas internas de la seguridad y mantenimiento del Data Center
			el encargado debe tomar decisiones en los aspectos de limpieza, y ciclo de mantenimiento de los equipos
	Contaminantes de gases y/o partículas	cotejar la calidad de aire	verificar que el área del Data center este fuera de presencia de los contaminantes suspendidos en el aire
8	Filtraciones de agua (lluvias, tuberías averiadas), inundación entre otros	Verificar los sistemas de protección y las medidas contra las filtraciones e inundaciones	desarrollar procedimientos de emergencia para inundaciones
			revisar las instalaciones de agua en los ambientes colindantes del Data Center
			Tener disponibles equipos de bombeo o extractores de agua
			Preparar bolsas de arena para las inundaciones
			mantener limpio el alcantarillado cercano al Data Center
	Huelgas y vandalismo	tener y reforzar el sistema la seguridad en el control de acceso	Asegurar de que los personales de seguridad estén disponibles en las entradas de la institución
			desarrollar procedimientos de emergencia para desórdenes civiles y eventos relacionados.
			Instalar cámaras de seguridad que pueden grabar eventos dentro y fuera del edificio.

9	Presencia de humedad	contar con los dispositivos sensor de Humedad	Contar con quipo sensor de humedad
			Control los dispositivos de humedad con monitoreo remoto
			verificar techos y paredes
10	Tormentas/rayos	Verificar el equipo pararrayo. Puesta a tierra de los equipos	las instalaciones de los quipos deben ser con puesta a tierra
			Revisar las características del proveedor de los equipos
			verificar el equipo de pararrayo este operativo
	Documentación insuficiente del cableado	Capacitación del personal de trabajo y verificar las instalaciones según normas.	Contar con las capacitaciones del personal
			el buen etiquetado de los equipos y las instalaciones

Medidas de control general y específicos para minimizar los riesgos de la Seguridad Física en el Data Center del Hospital Regional de Ayacucho.

A.2. Posteriormente de haber ejecutado la evaluación con los controles de la NTP-ISO/IEC 17799 se concluye:

Que el Data Center del hospital Regional de Ayacucho cumple con la categoría 9.1 (**Áreas seguras**) del Dominio 9 con los siguientes controles 9.1.2 (50%), 9.1.4(50%), 9.1.5 (100%) y 9.1.6 (75%) estos resultados se pueden considerar como niveles de seguridad aceptables. Y considerar no aceptable el control 9.1.1 (20%)

Y en la Categoría 9.2. (**Seguridad de los Equipos**) del Dominio 9 en los siguientes controles 9.2.2 (50%), 9.2.3 (50%), 9.2.4 (63%) y 9.2.7 (100%). Considerados como aceptables. En tanto los controles 9.2.1 (16.67%) y 9.2.6 (25) considerados no aceptables.

A.3. Después de haber realizado la evaluación con el COBIT 5.0 se concluye:

De los 17 criterios establecidos por COBIT 5.0 el Data Center del Hospital Regional de Ayacucho se tiene los siguientes resultados en Dominio: Evaluar, Orientar y Supervisar (Gobierno)-EDM (10%), Alinear, Planificar y Organizar (Gestión)-APO(30%), Construir, Adquirir e Implementar (Gestión)-BAI (0%) y en Entregar, dar Servicio y Soporte (Gestión) – DSS (12.50%) estos resultados presentan un escenario de seguridad física no satisfactorio, para lo cual requiere implementarse acciones de corrección de acuerdo a las recomendaciones mencionadas anteriormente.

B. RECOMENDACIONES:

B.1. Recomendaciones generales NTP-ISO/IEC 17799:2007 y COBIT 5.0:

Implementar en su totalidad los controles de Seguridad Física del Data Center del Hospital Regional de Ayacucho según NTP-ISO/IEC 17799; este código de buenas prácticas está orientado a uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799: 2014 EDI. TECNOLOGIA DE LA INFORMACIÓN. CODIGO DE BUENAS PRACTICAS PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION." en entidades del Sistema Nacional de Informática RESOLUCIÓN MINISTERIAL N° 224-2004-PCM.

Implementar en su totalidad los procesos de COBIT 5.0 concernientes a la Seguridad Física, esta implementación contribuirá con la administración y el control óptimo de la seguridad Física del Data Center del Hospital Regional de Ayacucho.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

a) De acuerdo al marco teórico del capítulo II, se logró implementar los procedimientos de auditoría en seguridad física utilizando la norma NTP-ISO/IEC 17799 y el marco de control de COBIT 5.0, usando técnicas e instrumentos sustentados en el capítulo III sección 3.4 se ha logrado identificar los principales activos físicos que están involucrados en la auditoría de seguridad física, cuyos resultados se muestran en el capítulo IV en la Tabla N° 7.

b) De acuerdo al marco teórico del capítulo II, sección 2.2.1, seguridad física, sección 2.2.3 Activo Físico, Amenaza y Riesgo, sección 2.2.4 Impacto, sección 2.2.9 Análisis de Riesgo, sección 2.3 metodología para realizar auditoría, usando técnicas e instrumentos de la sección 3.4, se ha logrado identificar las amenazas y riesgos más comunes en la auditoría de seguridad Física del Data Center y determinar el impacto en la seguridad física cuyos resultados se muestran en el capítulo IV en la Tabla N° 9, 10 y 11.

c) Con la evaluación del diagnóstico situacional de la seguridad Física del Data center del Hospital Regional de Ayacucho se logró identificar controles tanto de estandarización y normalización que se deben de tener en cuenta al planificar el diseño de un Data Center, lo cual ayudará a futuras investigaciones e implementación de un Data Center.

5.2 RECOMENDACIONES

a) Se recomienda que las entidades públicas de Ayacucho que pretenden implementar un Data Center adopten los lineamientos de la norma NTP-ISO/ lEC 17799, y las recomendaciones del estándar internacional TIER para obtener un buen diseño e implementación de un Data Center.

b) Como parte de la seguridad física del Data center, se recomienda generar conciencia de seguridad física en los funcionarios y trabajadores del establecimiento de Salud, mediante capacitaciones y charlas informativas.

BIBLIOGRAFÍA

ABB Review. (2012). Centro de datos. *La revista ABB*, 9-10.

Aguilera, P. (2010). *Seguridad Informática.* Madrid, España: Edilex, S.A.

Aguirre, D. S., & Palacios, J. C. (2014). *Evaluacion técnica de seguridades del Data Center del Municipio de Quito según las Normas ISO/IEC 27001:2005 SGSIE ISI/IEC 27002:2005.* Sangolqui.

Areitio, J. (2008). *Seguridad de la Información. Redes, informática y sistemas de información.* Madrid, España: Paraninfo.

Ary, W. (1996). *Metodología de la Investigacion.* madrid, España: Roalg.

Asociación Española de Normalización. (marzo de 2010). *Glosario de Seguridad*. Obtenido de http://www.cnis.es/glosario-seguridad/

Baldeón, M., & Coronel, C. (2012). *Plan maestro de seguridad informática con lineamiento de la norma ISO 27002.* Tesis de grado, Escuela politécnica del ejército vicerrectorado de investigación y vinculación con la colectividad, Departamento de ciencias de la computación maestría en gerencia de sistemas, Sangolqui.

Bernal Torres, C. A. (2010). *Metodología de la Investigación* (Tercera ed.). (O. F. Palma, Ed.) Colombia: Pearson Educación de Colombia Ltda.

Calderero hernandez, J. F., & Bernardo Carrasco, J. (2000). *Aprendo a Investigar en Educación.* ES: Rialp.

Chamorro, V. L. (2013). *Plan de seguridad de la información basado en el estándar iso 13335 aplicado a un caso de estudio.* Proyecto, ESCUELA POLITÉCNICA NACIONAL, Quito. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/5617

Chávez de Paz, D. (s.f). *Conceptos y Técnicas de Recolección de Datos en la Investigación Jurídico Social.* Universidad Nacional mayor de San Marcos.

Chavez, N. (2007). *Introducción a la investigación educativa.* Madrid: Gráfica gonzáles.

Chicano, E. (2015). *Auditoría de seguridad informática. IFCT0109.* IC Editorial.

Cilleros, D. (2012). *Seguridad en Data Centers: infraestructura y prevención.* Proyecto de Fin de Carrera, Universidad Carlos III, Madrid.

Cliatec. (2018). *Cliatec 360 Data Center*. Obtenido de https://cliatec.com/infraestructura-y-auditoria-de-data-center-la-mayoria-de-los-data-center-estan-obsoletos/

Consejo Superior de Administración Electrónica de España. (2012). *Magerit 3.0 Metodologia de Análisis y Gestión de Riesgos de los Sistemas de Información.* (M. d. Públicas, Ed.) Madrid.

Córdoba, M. (2003). *Estadpistica descriptiva e inferencial.* Lima, Perú: Moshera S.R.L.

Costas, J. (2011). *Seguridad y alta disponibilidad.* Madrid: RA-MA.

Date IT services. (6 de Noviembre de 2017). *Blog ITSD*. Obtenido de https://itservicesd.com/blog/2017/11/06/data-center/

Dávila Cervantes, J. A., & Ramírez Viteri, C. F. (2018). *Diseño de un Centro de Datos para la empresa isistem.* Trabajo de Titulacion, UDLA Facultad de Ingenería y Ciencias Aplicadas.

De Pablos, C., López-Hermoso, J. J., Martín-Romo, S., Medina, S., Montero, A., & Nájera, J. J. (2008). *Dirección y gestión de los sistemas de información de la empresa* (Segunda ed.). Madrid: Esic Editorial.

Goal's. (2014). *Goal's Infromation Networks Tech*. Obtenido de http://www.goalsnet.net/productos/data-center/auditoria-de-centros-de-datos/

Gobierno de España, Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método, Libro II - Catálogo de Elementos y Libro III - Guía de Técnicas.* (M. d. Administraciones, Ed.) Madrid, España. Obtenido de http://administracionelectronica.gob.es/

Gómez, J. A. (2011). *Redes locales.* Editex.

González, M. (2015). *Auditoría de información y de conocimiento en las organizaciones.* Tesis Doctoral, Universidad de la habana , De Biblioteconomía y Documentación de la Universidad de Granada, Granada.

Google. (2018). *Centros de Datos*. Obtenido de https://www.google.com.au/about/datacenters/

Govindan, M. (2007). *Control Interno, Auditoría y Seguridad Informática* (Vols. II-IV). España.

Hernández, R., Fernández, C., & Baptista, M. d. (2010). *Metodología d ela investigación.* México: McGRAW-HILL .

Hevada, F. (2007). *Gobierno de las Tecnologías y Sistemas de Información.* Madrid: ES. RA-MA.

Huerta Villalón, A. (2 de octubre de 2000). *Seguridad en Unix y Redes.* Obtenido de Versión 1.2 Digital - Open Publication License v.10 o Later: https://www.google.com/url?sa=t&source=web&rct=j&url=http://seguridadinformatica.wikidot.com/seguridad-fisica&ved=2ahUKEwj22s7kv5DkAhVwIrkGHT9QD00QFjACegQIDhAI&usg=AOvVaw20RsNw5V8e3I_rCv_mBSS4

Huerta, M. (2015). *Procedimiento para la Auditoria en seguridad fisica del Data Center en Municipalidad Provincial de Huamanga.* Tesis de Grado, Universidad de San Cristobal de Huamanga, Ayacucho, Ayacucho.

Hurtado, L. I., & Toro, G. J. (2005). *PARADIGMAS Y METODOS DE INVESTIGACION en tiempos de cambio* (Quinto ed.). Venezuela : Episteme Consultores Asociados C. A. Obtenido de https://epinvestsite.files.wordpress.com/2017/09/paradigmas-libro.pdf

ISACA. (2012). *COBIT 5.0, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Impreso en los Estados Unidos de America. Obtenido de www.isaca.org/COBITuse.

ISO 27001:2013. (Marzo de 2015). *Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

ISO/IEC - INDECOPI. (2014). *NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001* (Segunda ed.). (R.0129-2014/CNB-INDECOPI, Ed.) Lima.

ISOTools Excellence. (6 de Octubre de 2015). *Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Recuperado el 2019, de https://www.pmg-ssi.com/2015/10/la-norma-iso-27001-version-2013/

ISOTools EXCELLENCE. (s.f). La normaISO 27001 Aspectos clave de su diseño e implantación. Recuperado el 2019, de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Llerena, C. A., & Navarro, J. R. (2013). *FORMULACIÓN DE UNA GUÍA DE AUDITORIA PARA LA INFRAESTRUCTURA FÍSICA DE LOS CENTROS DE DATOS DE LAS ENTIDADES PÚBLICAS DEL ECUADOR BASADO EN MARCOS DE REFERENCIA DE TI.* Tesis de Grado, SANGOLQUI.

Loor, A. A., & Espinoza, V. A. (2015). *Auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la espam mfl.*

Lovos, F. D. (s.f). Seguridad Física y Lógica en centros de cómputo. *Auditoria de sistemas computarizados*.

Martínez, Y. (2012). Auditoria en Informática. *CU. Revista de Ingeniería, VI*(2), 14.

Marulanda, H. (2014). *Evaluación mediante el estándar ISO 27001 de la seguridad física y lógica de la infraestructura tecnológica de la clínica san josé s.a.s de la ciudad de Barrancabermeja – Santander.* Tesis de Grado, Universidad Francisco de Paula Santander Ocaña.

Morlano, G. (2012). Seguridad Informática, Matanzas. *CU. Revista de Arquitectura e Ingeniería, VI*(2), 1-14.

Mtnet. (2018). *Blog de TI* . Obtenido de https://www.mtnet.com.mx/blog/seguridad-fisica-en-el-data-center-las-cuatro-capas/

Muñoz, C. (2012). *Auditoría en sistemas computacionales.* Naucalpan de juarez, Mexico: Pearson educacion.

Navarro, E. (2005). *Manual de dictámenes y peritajes informáticos* (Segunda ed.). Madrid, España: DIAZ DE SANTOS.

Nogueira, J. E. (2014). *Procedimientos para la auditoría física y medio ambiental de un Data.* Lima.

NTP - ISO/IEC 17799 . (2007). *tecnología de la información.Código de buenas prácticas para la gestión de la seguridad de la información.* Presidencia del Consejo de Ministros – Gobierno del Perú – ONGEI, Lima.

Piattini, M. G., & Del peso, E. (2001). *Auditoria Infomática un enfoque práctico.* Madrid: Alfaomega Ra-ma Grupo editos S.A.

Ramió, J. (Marzo de 2003). *Seguridad Informática y Criptografía.* Universidad Politécnica de Madrid, Madrid.

Ramirez, G., & Álvarez, E. (2003). *Auditoría A La Gestión De Las tecnologías Y Sistemas De información.* Recuperado el Diciembre de 2018, de http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/vol6_n1/pdf/auditoria.pdf

Roa, J. F. (2013). *Seguridad informática.* Madrid: McGraw-Hill.

Seoane, C., Saiz, A. B., Fernández, E., & Fernández, L. (2010). *Seguridad Informática.* Madrid, España: McGraw-Hill.

Supo, J. (s.f). *Taxonomía de la investigación.* México.

Tamayo y Tamayo, M. (2004). *Diccionario de la Investigacion Científica* (Segunda ed.). Mexico: Noriega editores Limusa.

Thomas, P. (2010). *Information Security Risk Analysis* (Tercera ed.).

Tongo, Y. Y. (2017). *Diagnóstico situacional del Data Center bajo cumplimiento Normativo Y de Estándar en el Hospital Ii Essalud De Huaraz.* UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE, Huaraz.

Tupia, M. (2010). *Administración de la seguridad de información.* Lima: Graficar.

Universidad Juárez Autónoma de Tabasco. (2006). *Avances en Informática y Sistema Computacionales Tomo I CONAIS.* Tabasco, México.

Whitten, J. L. (2008). *Analisis y diseño de sistemas de informacion* (Tercera ed.). Mexico: McGraw-Hill.

ANEXOS

ANEXO A

Tabla A. 1
Matriz de Operacionalización de la Variable Seguridad Física

VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	INSTRUMENTO
Seguridad Física	**Activo Físico**	**Inventario de los activos físicos**	¿Qué activos físicos del Data center son importantes para que la institución alcance sus objetivos y estén establecidos con los objetivos del Hospital Regional de Ayacucho?	• Ficha de observación. • Cuestionario de encuestas.
		Ubicación de los activos físicos	¿Cómo deben estar ubicados los activos físicos en un Data Center y que garanticen el buen funcionamiento del mismo?	• Cuestionario de encuestas. • Ficha de análisis documental. • Cuestionario de entrevistas
		Confidencialidad	¿Cómo la difusión sin el consentimiento no autorizado de un activo físico puede afectar su confidencialidad del área?	• Ficha de análisis documental
		Integridad	¿Cómo la alteración natural o sin el consentimiento autorizado de un activo físico puede afectar su integridad del área?	
		Disponibilidad	¿De qué manera una pérdida, falla técnica de un activo físico puede afectar la disponibilidad y los servicios que brinda el Data Center?	
	Amenazas	**Identificación de las amenazas de activos físicos**	¿Cuáles son las amenazas que existen con los activos físicos del Data Center?	• Ficha de análisis documental

	Probabilidad de riesgo	¿Cuál es la probabilidad de riesgo se materialice la amenaza?	• Ficha de análisis documental
	Análisis de amenazas	¿Qué amenazas se ha identificado para los activos a los que está expuesto los activos físicos internos y externos? ¿A qué amenazas están expuestos los activos físicos?	• Ficha de análisis documental
Riesgo	**Identificar los riesgos de los activos físicos**	¿A qué riesgos están expuestos los activos físicos internos y externos?	• Ficha de análisis documental
	Impacto	¿Qué daño causaría sobre el activo físico la materialización de la amenaza?	• Ficha de análisis documental
	Análisis de Riesgo	¿Qué procesos de tratamiento de riesgos se va a seleccionar?	• Ficha de análisis documental
	Probabilidad	¿Cuál es la probabilidad de que se materialice la amenaza?	-Ficha de análisis documental
Criterios de Seguridad	**Criterios De Seguridad Física Basados En NTP-ISO/IEC 17799**	¿Cuáles son los criterios a ser aplicados dentro de una Auditoría a la Seguridad Física que permita realizar de forma correcta la auditoria del Data Center del Hospital Regional de Ayacucho?	• Cuestionario de encuestas • Ficha de análisis documental
	Criterios De Seguridad Física Basados en COBIT 5.0		
	Roles y responsabilidades	¿Cuáles son los roles y responsabilidades de los usuarios que administran el Data center?	• Cuestionario de entrevistas • Ficha de análisis documental

ANEXO B:

CONOCIMIENTO PRELIMINAR DEL DATA CENTER DEL HRA

DATOS GENERALES		ENTIDAD
Nombre de la Institución	**:**	Hospital Regional de Ayacucho
Área responsable	**:**	Área de Estadística e Informática
Área a auditar	**:**	Área de Data Center
Administrador del Data Center	**:**	Jefe del Área-Wilber Aguirre Landeo
Auditor	**:**	Bach. Vilca Dipaz Abel

Materiales para la ejecución de la auditoría: carpeta de trabajo, cámara digital.

Entrevista realizada al administrador del Data Center:

¿Cuál es el soporte del Data Center al Hospital Regional de Ayacucho? ¿Su funcionamiento es 24 horas del día, los 7 días de la semana y las 365 dial al año?

¿En cuanto a la Seguridad Física, Existen políticas, procedimientos formales y normas de acceso en el Data Center?

¿Se tiene la documentación sobre la construcción e instalaciones del Data Center?

¿Las contratas que se realiza en los procesos de mantenimiento preventivo y correctivo en el Data Center? ¿estas cuentan con seguros de riesgo?

ANEXO C:

CUESTIONARIO PARA LA ENTREVISTA

Nombre de la Organización:
……...
Área a entrevistar:
……
Dirigido:
……
Ciudad:
……
Dirección:
……
Fecha: ……/……/……

Tema de Investigación:

……..

Objetivo:

…….....

…….

1). ¿Existen políticas y procedimientos formales de Seguridad Física del Data Center del Hospital Regional de Ayacucho?

2). ¿Cómo se sociabiliza con los usuarios estas políticas y procedimientos?

3). ¿En cuanto a la documentación de las políticas y procedimientos, cuáles son los mecanismos de seguridad con la que se le da la salvaguarda?

4). ¿Para Las documentaciones de las políticas y procedimientos de seguridad del Hospital Regional de Ayacucho, cuáles son las condiciones de ambiente en las cuales están almacenadas?

5). ¿Existe un área específica para la seguridad física del Data Center (Área)?

6). ¿Cuáles son los procedimientos de acceso al Data Center Hospital Regional de Ayacucho?

7). ¿Se realiza el monitoreo y revisión de las bitácoras, de ser así cada que tiempo se realiza?

8). ¿Se evalúa el reporte de accesos al Data Center, de ser así este monitoreo con qué frecuencia se realiza?

9). ¿Se cuenta con sensores de Control ambiental para él Data Center?

10). ¿Se cuenta con políticas y procedimientos para elegir a los proveedores?

ANEXO D

D.1. CRITERIOS DE SEGURIDAD FÍSICA BASADOS EN NTP-ISO/IEC 17799 - DATA CENTER DEL HRA

De las directrices y controles presentados en el estándar NTP-ISO/IEC 17799:2007, se toma en cuenta la cláusula; Seguridad física y Ambiental (entorno), Domino 9. Los criterios de seguridad Física para el Data Center, definidos según esta norma son:

Tabla D. 1
Criterios de Seguridad Física Basados en NTP-ISO/IEC 17799 - Data Center del HRA

Dominio	**9. SEGURIDAD FÍSICA Y DEL ENTORNO (AMBIENTAL)**
Criterio	**9.1 Áreas Seguras** Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.
Control	**9.1.1 Perímetro de seguridad Física** Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados para proteger el área.
Guía de implementación. se debe considerar las siguientes directrices:	**f)** El perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física. Los muros externos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados; **g)** Se debería instalar un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería restringir sólo al personal autorizado; **h)** Las barreras físicas se deberían extender, si es necesario, desde el suelo real al techo real para evitar entradas no autorizadas o contaminación del entorno; **i)** Todas las puertas para incendios del perímetro de seguridad deberían tener alarma, ser monitoreadas y probadas; **j)** Se debe instalar sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales
Control	**9.1.2 Controles físicos de entradas** Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado

Guía de implementación. se debe considerar las siguientes directrices:	a) Las visitas a las áreas seguras se deberían supervisar, a menos que el acceso haya sido aprobado previamente, y se debe registrar la fecha y momento de entrada y salida. Los visitantes sólo tendrán acceso para propósitos específicos; b) Se debería controlar y restringir sólo al personal autorizado el acceso a la información sensible y a los recursos de su tratamiento; usar controles de autenticación, mantener un rastro auditable de todos los accesos; c) Se debería exigir a todo el personal que lleve puesta alguna forma de identificación visible y se le pedirá que solicite a los extraños no acompañados y a cualquiera que no lleve dicha identificación visible, que se identifique;
Control	**9.1.4 Protección contra amenazas externas y ambientales** Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana, del Data Center del Hospital Regional de Ayacucho.
Guía de implementación. se debe considerar las siguientes directrices:	**d)** Los materiales peligrosos y combustibles se deberían almacenar en algún lugar distante de las áreas seguras; **e)** El equipo y los medios de respaldo deberían estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal; **f)** Equipo apropiado contra incendio debe ser provisto y ubicado adecuadamente
Control	**9.1.5 El trabajo en el Data Center** Se debería diseñar y aplicar protección física y pautas para trabajar en el área de Data Center
Guía de implementación. se debe considerar las siguientes directrices:	**c)** Debería evitar el trabajo no supervisado en áreas seguras tanto por motivos de salud como para evitar oportunidades de actividades maliciosas; **d)** No se debería permitir la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial.
Control	**9.1.6 Acceso público, áreas de carga y descarga** Se deberían controlar las áreas de carga y descarga, y si es posible, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.
Guía de implementación. se debe considerar las siguientes directrices:	**a)** deberían restringir los accesos al área de carga y descarga desde el exterior únicamente al personal autorizado e identificado; **b)** El área de carga y descarga se debería diseñar para que los suministros puedan descargarse sin tener acceso a otras zonas del edificio;
Criterio	**9.2 Seguridad de los equipos** Evitar pérdidas, daños o comprometer los activos, así como la interrupción de las actividades de la organización.
Control	**9.2.1 Instalación y protección de equipos** El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.

Guía de implementación. se debe considerar las siguientes directrices:	d) Los controles deben ser adoptados para minimizar los riesgos de posibles amenazas como robo, incendio, explosivos, humo, agua (o fallo de suministro), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas y vandalismo; e) La organización debería incluir en su política cuestiones sobre fumar, beber y comer cerca de los equipos de tratamiento de información; **f)** Se deberían vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información;
Control	**9.2.2 Suministro eléctrico** Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo.
Guía de implementación. se debe considerar las siguientes directrices:	f) Todas las instalaciones de apoyo, como la electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado debe ser adecuado; g) Se recomienda instalar un Sistema de Alimentación Ininterrumpida (U.P.S.) para apoyar un cierre ordenado o el funcionamiento continuo de los equipos que soporten operaciones críticas del área; h) Además, se deberían instalar interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia; i) El suministro de agua debe ser estable y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados); j) Los equipos de telecomunicación deben ser conectados al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz
Control	**9.2.3 Seguridad del cableado** Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.
Guía de implementación. se debe considerar las siguientes directrices:	f) Las líneas de energía y telecomunicaciones en el Data Center, se deberían enterrar, cuando sea posible, o adoptarse medidas alternativas de protección; g) Se deberían separar los cables de energía de los de comunicaciones para evitar interferencias; h) Cables claramente identificados y marcas de equipo deben ser utilizadas con el fin de minimizar errores de manejo como el de parchar cables de una red incorrecta; i) Una lista documentada de parches debe utilizarse con el fin de reducir la posibilidad de errores; j) se deberían considerar medidas adicionales como: uso de rutas o de medios de transmisión alternativos; uso de cableado de fibra óptica; uso de un escudo electromagnético para proteger los cables, entre otros.
Control	**9.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.
Guía de implementación. se debe	e) Los equipos se deberían mantener de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del suministrador;

considerar las siguientes directrices:	f) Sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y servicio de los equipos; g) Se deberían registrar documentalmente todos las fallos, reales o sospechados, así como todo el mantenimiento preventivo y correctivo; h) Se debería implementar controles apropiados cuando el equipo es programado para mantenimiento, tomando en cuenta si este mantenimiento es realizado por personal interno o externo del área; donde sea necesario, debe despejarse la información sensible del equipo;
	9.2.6 Seguridad en el rehúso o eliminación de equipos
Control	Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.
Guía de implementación. se debe considerar las siguientes directrices:	c) Los dispositivos de almacenamiento con información sensible se deberían destruir físicamente o la información debe ser destruida, borrada o sobrescrita usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato; d) Los dispositivos dañados que contienen data sensible pueden requerir una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.
	9.2.7 Retiro de la propiedad
Control	El equipo, información o software no debe ser sacado fuera del local sin autorización
Guía de implementación. se debe considerar las siguientes directrices:	e) El equipo, información o software no debe ser sacado fuera del local sin autorización; f) Los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos deben ser claramente identificados; g) Los tiempos límite para el retiro de equipos deben ser fijados y el retorno del equipo verificado para asegurar la conformidad; h) El equipo debe ser registrado, si es necesario y apropiado, cuando este sea removido fuera del local, así como cuando sea devuelto.

D.2. CRITERIOS DE SEGURIDAD FÍSICA BASADOS EN COBIT 5.0 – DATA CENTER DEL HRA

Se define los criterios para una auditoría en seguridad física de un Data Center, basados en los dominios de COBIT 5.0 y sus respectivos objetivos de control seleccionados:

Tabla D. 2
Criterios de auditoría física y ambiental de Data Center según COBIT 5.

Dominio	**Evaluar, Orientar y Supervisar (Gobierno)-EDM**
	Asegura que los objetivos del Data Center sean logrados, evaluando las necesidades de los interesados
Procesos	**EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno**
	Verificar la existencia de un gobierno de seguridad física y ambiental en el Data Center de la institución
	EDM05 Asegurar la transparencia hacia las partes interesadas
	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de las TI de la empresa son transparentes
Objetivo	**EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.**
	Verificar la existencia de contratos que detallen los niveles de seguridad que el Data Center ofrecerá a los clientes.
Dominio	**Alinear, Planificar y Organizar (Gestión)-APO**
	Este dominio proporciona la dirección para la entrega de soluciones y la entrega de servicios
Proceso	**APO01 Gestionar el Marco de Gestión de TI**
	Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.
Objetivos	**APO01.02 Establecer roles y responsabilidades.**
	Verificar el establecimiento de roles y responsabilidades en seguridad física del Data Center del HRA.
	APO01.07 Gestionar la mejora continua de los procesos.
	Verificar la ejecución de capacitaciones al personal encargado sobre las consideraciones de seguridad física del Data Center, cómo afectan a las operaciones del Hospital Regional de Ayacucho y las acciones a tomar en situaciones de riesgo.
Proceso	**APO07 Gestionar los Recursos Humanos**
	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.
Objetivo	**APO07.01 Mantener la dotación de personal suficiente y adecuada.**
	Verificar la adecuada proporción entre recursos humanos y proveedores con respecto a los servicios que se ofrecen.
Proceso	**APO10 Gestionar los Proveedores**
	Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos de equipos y servicios para el Data Center
Objetivo	**APO10.03 Gestionar contratos y relaciones con proveedores.**
	Verificar que los contratos con terceros o proveedores por lo menos deben incluir acuerdos de seguridad, acuerdos de confidencialidad**.**
Proceso	**APO12 Gestionar el Riesgo**

	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa
Objetivo	**APO12.05 Definir un portafolio de acciones para la gestión de riesgos del Data Center.**
Dominio	**Construir, Adquirir e Implementar (Gestión)-BAI**
	La gerencia con este dominio pretende cubrir, que los nuevos proyectos generen soluciones que satisfagan las necesidades del Data Center
Proceso	**BAI03. Gestionar la Identificación y Construcción de Soluciones.**
	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes.
Objetivos	**BAI03.07 Preparar pruebas de la solución**
	Verificar la existencia de un plan de pruebas de soluciones en seguridad física y ambiental del Data Center.
	BAI03.08 Ejecutar pruebas de la solución
	Verificar si se han ejecutado las pruebas de soluciones en seguridad física de forma continua, identificando, registrando y dando prioridad a los errores y los problemas detectados durante las pruebas.
Proceso	**BAI06 Gestionar los Cambios**
	Gestiona todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura**.**
Objetivo	**BAI06.02 Gestionar cambios de emergencia.**
	Verificar la existencia de mecanismos de emergencia que controlen el mantenimiento de los equipos del Data Center
Dominio	**Entregar, dar Servicio y Soporte (Gestión) - DSS**
	Es lograr que los servicios de TI se entreguen de acuerdo con las prioridades del Data Center, la optimización de costos, asegurar que la fuerza de trabajo utilice los sistemas de modo productivo y seguro, implantar de forma correcta la confidencialidad, la integridad y la disponibilidad.
Proceso	**DSS01 Gestionar Operaciones**
	Entregar los resultados del servicio operativo de TI, según lo planificado
Objetivo	**DSS01.04 Gestionar el entorno.**
	Verificar el cumplimiento de requisitos de gestión ambiental.
Proceso	**DSS02 Gestionar las peticiones y los incidentes del servicio**
	Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.
Objetivos	**DSS02.04 Investigar, diagnosticar y localizar incidentes.**
	DSS02.05 Resolver y recuperarse de incidentes.
Proceso	**DSS04 Gestionar la Continuidad**
	Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.
Objetivos	**DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.**
	DSS04.07 Gestionar acuerdos de respaldo
Proceso	**DSS05 Gestionar Servicios de Seguridad**

	Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.
Objetivos	**DSS05.05 Gestionar el acceso físico a los activos de TI.**
	Verificar la existencia de mecanismos de autorización y restricción de acceso a los locales del Data Center
	DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
	Verificar la existencia de garantías que aseguren y protejan la seguridad física y ambiental del Data Center.
	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
	Verificar la existencia de herramientas de detección de intrusos para controlar el acceso no autorizado al Data Center.

ANEXO E

Tabla E. 1
Activos de un Data Center

ACTIVOS FISICOS QUE SE ENCUENTRAN EN UN DATA CENTER			
GRUPO	**EQUIPO PARA UNIDAD DE INFORMATICA**	**CANTIDAD**	**CARACTERISTICAS/DESCRIPCION**

Tabla para identificación de los activos físicos del Data Center.

Tabla E. 2
Tasación de los Activos

Nº	ACTIVOS DEL DATA CENTER	VALOR DEL ACTIVO

Tabla para la tasación de los activos físicos del Data Center

Tabla E. 3
Criterio para la tasación de activos

VALOR	SIGNIFICADO	CRITERIO ◆ DISPONIBILIDAD
1	Muy bajo	Daño irrelevante a efectos prácticos
2	Bajo	Daño menor
3	Moderado	Daño importante
4	Alto	Daño grave

5	Muy alto	Daño muy grave

Criterio de valoración de los activos según escala Likert. Fuente: (Chamorro, 2013)

Tabla E. 4

Cálculo de Probabilidad de ocurrencia de una amenaza frente a una vulnerabilidad del Data center

Nº	**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD DE OCURRENCIA D ELA AMENAZA**

Cálculo de Probabilidad de ocurrencia de una amenaza frente a una vulnerabilidad del Data Center del Hospital Regional de Ayacucho. Fuente: (Llerena & Navarro, 2013)

Tabla E. 5

Matriz de Riesgo

Matriz de Riesgos	Amenazas
Probabilidad de amenaza	
Activo **Impacto**	**Medición o valoración de Riesgo**

Matriz de riego de los activos físicos del Data Center de las amenazas. Fuente: (Llerena & Navarro, 2013)

ANEXO F

ILUSTRACIONES DE LOS ACTIVOS FÍSICOS DEL DATA CENTER-HOSPITAL REGIONAL DE AYACUCHO

Ilustración F. 1 vista general del Data Center

Ilustración F. 2 Tablero de distribución eléctrica

Ilustración F. 3 puerta del Data Center

Ilustración F. 4 Pasadizo al Data Center

Ilustración F. 5 Interior parte superior del ambiente

Ilustración F. 6 Cableado interior del ambiente

Ilustración F. 7 cableado del Rack

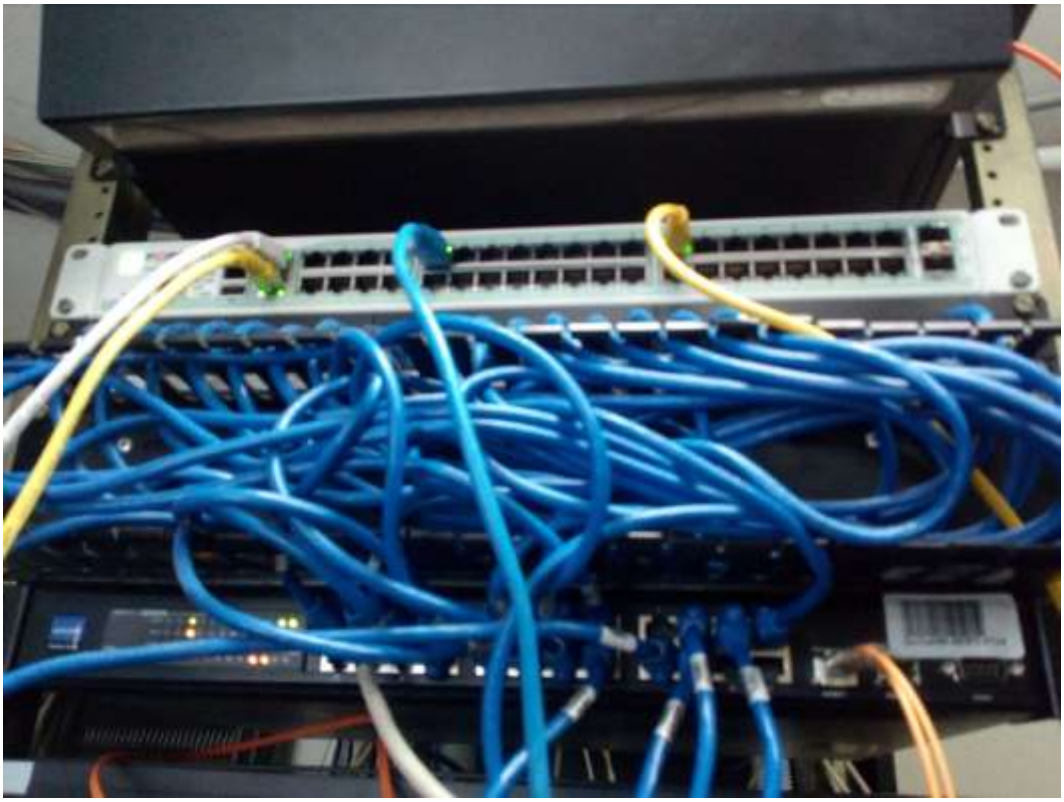


Ilustración F. 8 Cableado de servidores

Ilustración F. 9 Piso Data Center

Ilustración F. 11 Ups

Ilustración F. 10 Vista frontal de Rack y servidores

Ilustración F. 12 Aire acondiciona

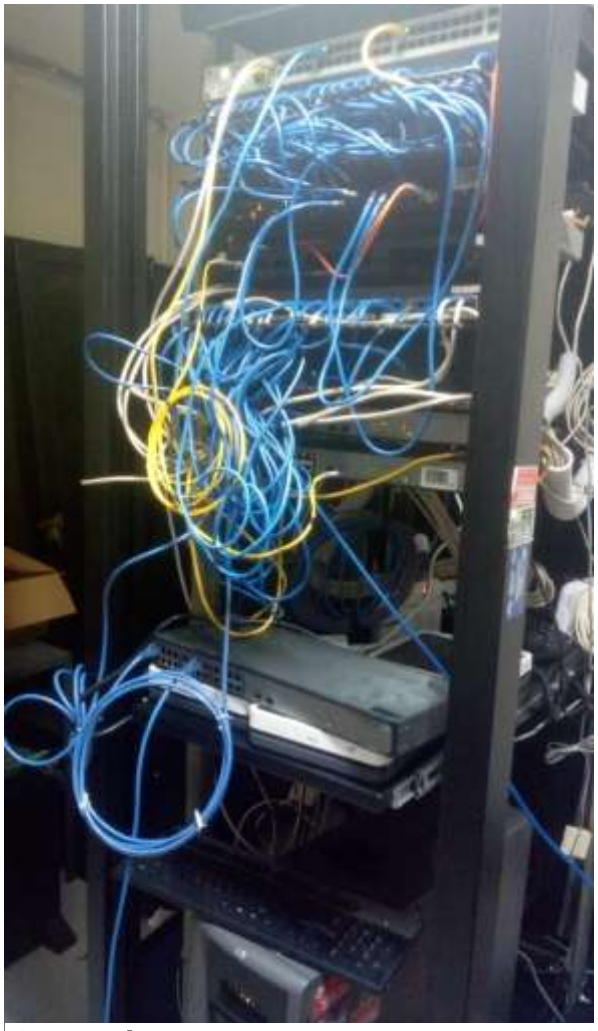


Ilustración F. 13 Vista parte posterior de cableado del rack

Ilustración F. 14 Entrevista al jefe del área de informática